Elliptische Kurven II
Vorlesung im Wintersemester 2000/2001

Michael Stoll

KAPITEL 1

Einführung

In diesem zweiten Teil der Vorlesung soll es um Elliptische Kurven über $\mathbb{Q}$ gehen, nachdem wir uns im ersten Teil hauptsächlich auf den Fall eines endlichen Grundkörpers beschränkt haben. Ein wesentliches Ziel dabei ist der Beweis des *Satzes von Mordell(-Weil)*. Er sagt aus, daß für eine Elliptische Kurve E über $\mathbb{Q}$ die Gruppe $E(\mathbb{Q})$ der rationalen Punkte eine *endlich erzeugte* abelsche Gruppe ist. Das bedeutet, daß man eine Zerlegung hat

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r \,,$$

wo $E(\mathbb{Q})_{\text{tors}}$ eine endliche abelsche Gruppe und r eine natürliche Zahl ist. Diese Zahl r heißt dann der *(Mordell-Weil-)Rang* von E.

Ein weiteres Ziel ist die Formulierung der *Vermutung von Birch und Swinnerton-Dyer*. Sie stellt einen Zusammenhang her zwischen dem Verhalten von E modulo allen Primzahlen und „globalen“ Invarianten von E, wie zum Beispiel $E(\mathbb{Q})_{\text{tors}}$ und dem Rang von E.

Beginnen möchte ich jedoch mit den wichtigsten Resultaten über Elliptische Kurven über den komplexen Zahlen. Zum einen ist diese Theorie schön und wichtig, und man sollte sie kennen. Zum anderen brauchen wir einen Teil davon sowieso, um eine der Invarianten (die sogenannte „reelle Periode“) zu definieren, die in der Birch–Swinnerton-Dyer-Vermutung auftreten.

KAPITEL 2

Elliptische Kurven über C

Sei E eine Elliptische Kurve über $\mathbb{C}$. Die Menge $E(\mathbb{C})$ ihrer Punkte wird beschrieben durch eine Gleichung in zwei Variablen. Wenn wir uns einen Moment auf den affinen Teil beschränken, dann haben wir eine Teilmenge von $\mathbb{C}^2$, die durch eine Gleichung beschrieben wird. Nach dem Satz über implizite Funktionen können wir lokal die Gleichung nach einer der beiden Variablen holomorph auflösen (die zu erfüllende Bedingung bedeutet gerade, daß E glatt ist), so daß $E(\mathbb{C})$ lokal aussieht wie ein Stück der komplexen Ebene $\mathbb{C}$. Das gilt für jeden affinen Teil von $E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$, so daß $E(\mathbb{C})$ insgesamt zu einer eindimensionalen komplexen Mannigfaltigkeit, einer sogenannten *Riemannschen Fläche* wird, ähnlich wie die Lösungsmenge einer oder mehrerer Gleichungen im $\mathbb{R}^n$ unter geeigneten Voraussetzungen eine (differenzierbare) reelle Mannigfaltigkeit bildet. Ebenso wie man auf differenzierbaren reellen Mannigfaltigkeiten Analysis treiben kann, kann man Funktionentheorie auf Riemannschen Flächen machen. Für eine anschauliche Kurzeinführung in diese Materie seien die letzten Kapitel des Buches von Jänich [**Jae**] empfohlen.

Diese Fläche $E(\mathbb{C})$ ist topologisch ein Torus. Da man einen Torus auch bekommt, wenn man in der Ebene Punkte identifiziert, deren Differenz in einem gegebenen Gitter (das ist eine additive Untergruppe, die von zwei linear unabhängigen Elementen erzeugt wird) liegt, ist das Hauptresultat dieses Kapitels vielleicht nicht mehr ganz so überraschend. Es sagt nämlich Folgendes.

SATZ 2.1. *Zu jeder Elliptischen Kurve E über $\mathbb{C}$ gibt es ein Gitter $\Lambda \subset \mathbb{C}$ und einen Isomorphismus $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ als Gruppen und als Riemannsche Flächen. Umgekehrt gibt es zu jedem Gitter $\Lambda \subset \mathbb{C}$ eine Elliptische Kurve E über $\mathbb{C}$ mit dieser Eigenschaft.*

Dabei ist $\mathbb{C}/\Lambda$ eine Gruppe als Faktorgruppe der additiven Gruppe von $\mathbb{C}$ nach dem Normalteiler Λ. Gleichzeitig ist $\mathbb{C}/\Lambda$ aber auch eine Riemannsche Fläche, da eine kleine Umgebung von $z + \Lambda \in \mathbb{C}/\Lambda$ genau so aussieht wie eine kleine Umgebung von $z \in \mathbb{C}$. (Die Topologie auf $\mathbb{C}/\Lambda$ ist die sogenannte Quotiententopologie. Sei $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ die kanonische Abbildung; dann ist $U \subset \mathbb{C}/\Lambda$ offen genau dann, wenn das Urbild $\pi^{-1}(U) \subset \mathbb{C}$ offen ist. Diese Topologie ist die feinste, die π stetig macht.)

1. Elliptische Funktionen

Wir beginnen mit dem zweiten Teil des obigen Satzes; wir gehen also aus von einem gegebenen Gitter Λ.

1.1. Gitter in C. Zunächst die fällige Definition.

DEFINITION 2.2. Ein *Gitter* $\Lambda \subset \mathbb{C}$ ist eine additive Untergruppe der Form

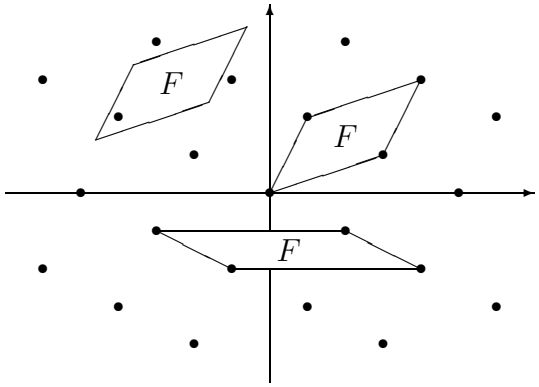
$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2\,,$$

wo $\omega_1, \omega_2 \in \mathbb{C}$ über $\mathbb{R}$ linear unabhängig sind (also eine Basis des $\mathbb{R}$-Vektorraumes $\mathbb{C}$ bilden).

Ein *Fundamentalparallelogramm* für Λ ist eine Menge der Form

$$F = \{a + t_1\omega_1 + t_2\omega_2 \mid t_1, t_2 \in [0,1]\}$$

mit $a, \omega_1, \omega_2 \in \mathbb{C}$, wo ω_1, ω_2 eine Basis für Λ bilden.



Beachte, daß so ein Gitter viele Basen hat: mit ω_1, ω_2 ist zum Beispiel auch $2\omega_1 + 3\omega_2, \omega_1 + 2\omega_2$ eine Basis.

LEMMA 2.3. *Sei $\Lambda \subset \mathbb{C}$ ein Gitter, $\pi : \mathbb{C} \longrightarrow \mathbb{C}/\Lambda$ die kanonische Abbildung und F ein Fundamentalparallelogramm für Λ. Dann ist $\pi : F \longrightarrow \mathbb{C}/\Lambda$ surjektiv. Insbesondere ist $\mathbb{C}/\Lambda$ kompakt.*

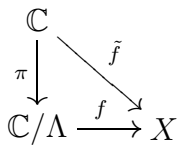
BEWEIS: Sei F durch a, ω_1, ω_2 gegeben wie in der Definition, und sei $z+\Lambda \in \mathbb{C}/\Lambda$ ein Element. Wir müssen zeigen, daß es ein $w \in F$ gibt mit $z + \Lambda = w + \Lambda$, d.h., $z - w \in \Lambda$. Dazu schreiben wir alles in der $\mathbb{R}$-Basis ω_1, ω_2 von $\mathbb{C}$: $z = z_1\omega_1 + z_2\omega_2$, $a = a_1\omega_1 + a_2\omega_2$ mit $z_1, z_2, a_1, a_2 \in \mathbb{R}$. Sei $n_1 = \lfloor z_1 - a_1 \rfloor$, $n_2 = \lfloor z_2 - a_2 \rfloor$; dann gilt $z = (a + t_1\omega_1 + t_2\omega_2) + (n_1\omega_1 + n_2\omega_2)$ mit $0 \le t_1, t_2 < 1$, also $z \in F + \Lambda$, was zu zeigen war.

Da F (als abgeschlossene und beschränkte Menge oder als Bild des kompakten Einheitsquadrats unter der stetigen Abbildung $(t_1, t_2) \mapsto a + t_1\omega_1 + t_2\omega_2$) kompakt ist, ist auch $\mathbb{C}/\Lambda$ als Bild von F unter der stetigen Abbildung π kompakt. □

Da (wie man sich ähnlich wie in obigem Beweis leicht überlegt) die einzigen Paare von Elementen eines Fundamentalparallelogramms F, die modulo Λ kongruent sind, auf gegenüberliegenden Seiten von F liegen, kann man den topologischen Raum $\mathbb{C}/\Lambda$ erhalten, indem man so ein F an den zwei Paaren gegenüberliegender Seiten zusammenklebt. Bei der ersten Verklebung entsteht ein Zylinder, bei der zweiten dann ein Torus.

Wir interessieren uns nun für meromorphe Funktionen auf der kompakten Riemannschen Fläche $\mathbb{C}/\Lambda$. Wir brauchen dafür aber nicht die Funktionentheorie auf Riemannschen Flächen zu entwickeln, denn es läßt sich alles auf die bekannte Funktionentheorie auf $\mathbb{C}$ zurückführen. Daß das so ist, liegt an der folgenden Bemerkung.

BEMERKUNG 2.4. Sei $\Lambda \subset \mathbb{C}$ ein Gitter mit kanonischer Projektion $\pi : \mathbb{C} \longrightarrow \mathbb{C}/\Lambda$. Dann liefert $f \mapsto f \circ \pi$ eine Bijektion zwischen Abbildungen $f : \mathbb{C}/\Lambda \longrightarrow X$ und Abbildungen $\tilde{f} : \mathbb{C} \longrightarrow X$ mit der Eigenschaft, daß $\tilde{f}(z+\omega) = \tilde{f}(z)$ gilt für alle $z \in \mathbb{C}$ und $\omega \in \Lambda$.



1.2. Elliptische Funktionen. Erste Eigenschaften. Obiger Bemerkung folgend, betrachten wir statt meromorpher Funktionen auf $\mathbb{C}/\Lambda$ meromorphe Funktionen auf $\mathbb{C}$, die bezüglich Λ (doppelt-)periodisch sind. Für die verwendeten Sätze aus der Funktionentheorie sei wiederum auf das Buch von Jänich [**Jae**] verwiesen.

DEFINITION 2.5. Sei $\Lambda \subset \mathbb{C}$ ein Gitter. Eine *elliptische Funktion* für Λ ist eine meromorphe Funktion $f : \mathbb{C} \longrightarrow \mathbb{C}$ mit $f(z+\omega) = f(z)$ für alle $z \in \mathbb{C}$, $\omega \in \Lambda$.

BEMERKUNG 2.6.

(1) Summe, Differenz, Produkt und Quotient zweier elliptischer Funktionen für Λ sind wieder elliptische Funktionen für Λ. Die Menge der elliptischen Funktionen für Λ bildet also einen Körper $\mathcal{M}(\Lambda)$. Dieser Körper enthält $\mathbb{C}$ als die konstanten Funktionen.
(2) Wenn ω_1, ω_2 eine Basis von Λ ist, dann ist die Periodizitätsbedingung äquivalent zu
$$f(z+\omega_1) = f(z+\omega_2) = f(z) \quad \text{für alle } z \in \mathbb{C}.$$
(3) Ist $0 \neq f \in \mathcal{M}(\Lambda)$, dann gibt es ein Fundamentalparallelogramm F für Λ, so daß f auf dem Rand ∂F keine Nullstellen oder Pole hat. (Zum Beweis betrachte ein F_0 mit $a = 0$. In der kompakten Menge $2F$ hat f nur endlich viele Nullstellen und Pole (sie können sich wegen des Identitätssatzes nicht häufen), also sind von allen $F = a + F_0$ mit $a \in F_0$ nur endlich viele ausgeschlosen.)

Nun könnte man fragen, warum wir nicht erst einmal holomorphe Funktionen betrachten. Die Antwort ist, daß es keine (interessanten) gibt.

LEMMA 2.7. *Eine holomorphe elliptische Funktion ist konstant.*

BEWEIS: Sei $f \in \mathcal{M}(\Lambda)$ holomorph. Dann ist f als stetige Funktion auf der kompakten Menge F beschränkt, wo F ein Fundamentalparallelogramm ist. Nach Lemma 2.3 gilt aber $f(\mathbb{C}) = f(F)$, also ist f überhaupt beschränkt und damit nach dem Satz von Liouville konstant. □

Eine nicht-konstante elliptische Funktion muß also mindestens einen Pol (modulo Λ) haben. Das ist aber nicht die einzige Einschränkung.

SATZ 2.8. *Sei $\Lambda \subset \mathbb{C}$ ein Gitter und $0 \neq f \in \mathcal{M}(\Lambda)$ eine elliptische Funktion. Sei weiter F ein Fundamentalparallelogramm für Λ, so daß f auf dem Rand ∂F keine Nullstellen oder Pole hat (siehe Bem. 2.6). Dann gilt:*

(1) $\displaystyle\sum_{z\in F} \operatorname{res}_z(f) = 0$;
(2) $\displaystyle\sum_{z\in F} \operatorname{ord}_z(f) = 0$;
(3) $\displaystyle\sum_{z\in F} z \cdot \operatorname{ord}_z(f) \in \Lambda$.

(Dabei ist $\operatorname{res}_z(f)$ das Residuum von f in z und $\operatorname{ord}_z(f)$ die Ordnung (d.h. Vielfachheit der Nullstelle oder negativ genommene Vielfachheit des Pols) von f in z. Da f in F nur endlich viele Nullstellen und Pole hat, sind die Summen endlich.)

BEWEIS: Der Beweis besteht jeweils in der Anwendung des Residuensatzes auf ein Integral $\int_{\partial F} g(z)\,dz$ mit einer geeigneten Funktion g. Der Integrationsweg ist dabei der entgegen dem Uhrzeigersinn orientierte Rand von F. Wenn F durch a, ω_1, ω_2 gegeben ist, dann gilt also

$$\begin{aligned}\int_{\partial F} g(z)\,dz &= \Big(\int_a^{a+\omega_1} - \int_{a+\omega_2}^{a+\omega_1+\omega_2}\Big) g(z)\,dz - \Big(\int_a^{a+\omega_2} - \int_{a+\omega_1}^{a+\omega_1+\omega_2}\Big) g(z)\,dz \\ &= \int_a^{a+\omega_1} \big(g(z) - g(z+\omega_2)\big)\,dz - \int_a^{a+\omega_2} \big(g(z) - g(z+\omega_1)\big)\,dz\,. \qquad (1.1)\end{aligned}$$

(1) Wir setzen $g = f$ in (1.1). Es folgt

$$2\pi i \sum_{z\in F} \operatorname{res}_z(f) = \int_{\partial F} f(z)\,dz = 0$$

wegen der Periodizität von f.

(2) Wir setzen $g = f'/f \in \mathcal{M}(\Lambda)$. Dann gilt $\operatorname{res}_z(g) = \operatorname{ord}_z(f)$, und wie eben folgt $\sum_{z\in F} \operatorname{ord}_z(f) = 0$.

(3) Hier nehmen wir $g(z) = z\,f'(z)/f(z)$; dann ist $\operatorname{res}_z(g) = z\cdot\operatorname{ord}_z(f)$. Allerdings ist g nicht mehr Λ-periodisch, sondern es gilt

$$g(z) - g(z+\omega) = -\omega\, f'(z)/f(z)$$

für $z \in \mathbb{C}$, $\omega \in \Lambda$. Mit (1.1) haben wir also

$$2\pi i \sum_{z\in F} z \cdot \operatorname{ord}_z(f) = -\omega_2 \int_a^{a+\omega_1} \frac{f'(z)}{f(z)}\,dz + \omega_1 \int_a^{a+\omega_2} \frac{f'(z)}{f(z)}\,dz\,.$$

Da f auf ∂F keine Pole oder Nullstellen hat, gibt es eine holomorphe Funktion h auf einer Umgebung der Strecke $[a, a+\omega_1]$ mit $\exp(h(z)) = f(z)$ auf dieser Umgebung. Es gilt dann $h' = f'/f$, also haben wir

$$\int_a^{a+\omega_1} \frac{f'(z)}{f(z)}\,dz = h(a+\omega_1) - h(a)\,,$$

und das muß $2\pi i$ mal eine ganze Zahl sein, weil

$$\exp(h(a+\omega_1) - h(a)) = f(a+\omega_1)/f(a) = 1$$

ist. Das andere Integral behandelt man ebenso. Insgesamt folgt

$$2\pi i \sum_{z\in F} z \cdot \operatorname{ord}_z(f) = -2\pi i\omega_2 n_2 + 2\pi i\omega_1 n_1$$

mit $n_1, n_2 \in \mathbb{Z}$, was zur Behauptung äquivalent ist. □

Teil (2) des Satzes zeigt, daß folgende Definition sinnvoll ist.

DEFINITION 2.9. Sei $0 \neq f \in \mathcal{M}(\Lambda)$. Dann heißt die Anzahl der Pole von f (mit Vielfachheit gezählt) in einem (jedem) Fundamentalparallelogramm, auf dessen Rand keine Pole oder Nullstellen von f liegen, die *Ordnung* von f. Die Ordnung ist auch gleich der Anzahl der Nullstellen (mit Vielfachheit gezählt).

Aus dem Satz folgt, daß es keine elliptischen Funktionen der Ordnung 1 gibt, denn ein einfacher Pol hat immer ein nicht-verschwindendes Residuum. Die einfachsten elliptischen Funktionen werden also Ordnung 2 haben und entweder einen zweifachen Pol mit Residuum 0 oder zwei einfache Pole bei $z + \Lambda$ und $-z + \Lambda$ mit entgegengesetzen Residuen haben. Wir werden im nächsten Abschnitt so eine Funktion der Ordnung 2 konstruieren.

Man kann sich allgemeiner die Frage stellen, wann es zu vorgegebenen Ordnungen $\operatorname{ord}_z(f)$, $z \in F$, eine elliptische Funktion gibt. Die Teile (2) und (3) des Satzes geben notwendige Bedingungen. Wir werden sehen, daß diese Bedingungen auch hinreichend sind.

ÜBUNGSAUFGABEN 2.1.

(1) Zeigen Sie, daß die diskreten additiven Untergruppen von $\mathbb{R}^2$ (oder allgemeiner, von $\mathbb{R}^n$) die Form $\mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_m$ haben, wobei $\omega_1, \ldots, \omega_m \in \mathbb{R}^2$ (bzw. $\mathbb{R}^n$) $\mathbb{R}$-linear unabhängig sind (insbesondere ist $m \leq 2$ (bzw. $m \leq n$)). Zeigen Sie weiter, daß eine solche Untergruppe $\Lambda \subset \mathbb{R}^n$ genau dann kokompakt ist (d.h. $\mathbb{R}^n/\Lambda$ ist kompakt), wenn $m = n$ ist.
(2) Sei $\Lambda \subset \mathbb{C}$ ein Gitter. Zeigen Sie:
   (a) Jedes Fundamentalparallelogramm für Λ hat denselben Flächeninhalt A.
   (b) Für $R \to \infty$ gilt
   $$\#\{\omega \in \Lambda \;\big|\; |\omega| \leq R\} = \frac{\pi}{A} R^2 + O(R)\,.$$
   (c) Es gibt $c > 0$, so daß für alle $R > 0$ gilt
   $$\#\{\omega \in \Lambda \mid R \leq |\omega| < R + 1\} \leq cR\,.$$
   (d) Für $s \in \mathbb{R}$ mit $s > 2$ konvergiert die Reihe $\sum_{\omega\in\Lambda\setminus\{0\}} |\omega|^{-s}$.
(3) Sei $\Lambda_4 = \mathbb{Z} + \mathbb{Z}i$ das Quadratgitter und $\Lambda_6 = \mathbb{Z} + \mathbb{Z}\rho$ mit $\rho = \frac{1}{2}(1 + \sqrt{3}i) = e^{\pi i/3}$ das Sechseckgitter. Zeigen Sie, daß $G_6(\Lambda_4) = 0$ und $G_4(\Lambda_6) = 0$. Erinnerung: $G_k(\Lambda) = \sum_{\omega\in\Lambda\setminus\{0\}} \omega^{-k}$.

1.3. Konstruktion von elliptischen Funktionen. Wir haben gesehen, daß ein möglicher Kandidat für eine einfachste nicht-konstante elliptische Funktion einen Pol zweiter Ordnung mit Residuum null in jedem Gitterpunkt hat. So eine Funktion sollte also zum Beispiel in jedem $\omega \in \Lambda$ den Hauptteil $(z - \omega)^{-2}$ haben.

Man wäre jetzt vielleicht versucht,

$$f(z) = \sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^2} \tag{1.2}$$

zu setzen; diese Funktion wäre offensichtlich Λ-periodisch. Dummerweise konvergiert aber die Reihe für kein $z \in \mathbb{C}$ absolut, denn für festes z ist der Term, über den summiert wird, von der Größenordnung ω^{-2}, und $\sum_{\omega\in\Lambda\setminus\{0\}} |\omega|^{-2}$ ist divergent, wie man aus der Übungsaufgabe 2.1, (2) schließen kann. Also muß man etwas tun, um die Konvergenz zu erzwingen: Man zieht einfach ω^{-2} ab und setzt

$$\wp(z) = \wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

Das ist die sogenannte *Weierstraßsche $\wp$-Funktion*. Der Term in der Summe ist jetzt

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{\omega^2-(z-\omega)^2}{\omega^2(z-\omega)^2} = \frac{2z\omega - z^2}{\omega^2(z-\omega)^2} = O(|\omega|^{-3}),$$

gleichmäßig für z in einem Kompaktum in $\mathbb{C}\setminus\Lambda$, also konvergiert die Reihe gegen eine in $\mathbb{C}$ meromorphe Funktion mit Polen nur in den Gitterpunkten von Λ mit Hauptteil $(z-\omega)^{-2}$. (Diese Methode mit den „konvergenzerzeugenden Summanden“ funktioniert übrigens in ähnlicher Weise immer — Zu einem Gebiet $U \subset \mathbb{C}$ gibt es stets eine auf U meromorphe Funktion mit vorgeschriebenen Hauptteilen in U, solange sich die vorgeschriebenen Pole in U nicht häufen. Das ist der Inhalt des *Satzes von Mittag-Leffler*.)

Nun haben wir also eine meromorphe Funktion $\wp$ mit den richtigen Polen. Ist $\wp$ auch elliptisch? Heuristisch würde man das vielleicht erwarten, denn wir haben zu unserem Λ-periodischen Ansatz (1.2) nur eine Konstante addiert. Allerdings verhalten sich unendliche Reihen ja oft kontraintuitiv; deswegen sollten wir uns nach einem ordentlichen Beweis umsehen. Man kann das relativ einfach anhand der Reihe sehen — für $\lambda \in \Lambda$ ergibt die Differenz $\wp(z+\lambda) - \wp(z)$ eine absolut konvergente Reihe, die nicht von z abhängt und deren Summe null ist. Eleganter ist aber der folgende üblicherweise angewandte Trick. Da die Reihe für $\wp$ kompakt konvergent ist, dürfen wir gliedweise differenzieren und erhalten

$$\wp'(z) = -2\sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^3},$$

woraus man sofort sieht, daß $\wp'$ elliptisch ist. Da die Ableitung von $\wp(z+\omega) - \wp(z)$ also verschwindet, muß diese Differenz konstant sein. Nun verwendet man, daß $\wp$ eine gerade Funktion ist (d.h. $\wp(-z) = \wp(z)$; das ist aus der Definition offensichtlich) und wertet obige Differentz bei $-\omega/2$ aus:

$$\text{const.} = \wp(-\omega/2+\omega) - \wp(-\omega/2) = \wp(\omega/2) - \wp(\omega/2) = 0.$$

Wir bezeichnen den Unterkörper der geraden Funktionen im Körper $\mathcal{M}(\Lambda)$ der elliptischen Funktionen mit $\mathcal{M}(\Lambda)^+$ und die Teilmenge der ungeraden Funktionen mit $\mathcal{M}(\Lambda)^-$. Wir haben mit obigen Überlegungen bereits den ersten Teil des folgenden Satzes gezeigt.

SATZ 2.10.

(1) $\wp_\Lambda \in \mathcal{M}(\Lambda)^+$ *ist eine gerade elliptische Funktion der Ordnung 2;*
$\wp'_\Lambda \in \mathcal{M}(\Lambda)^-$ *ist eine ungerade elliptische Funktion der Ordnung 3.*

(2) $\mathcal{M}(\Lambda)^+ = \mathbb{C}(\wp_\Lambda)$*, d.h., jede gerade elliptische Funktion ist eine rationale Funktion von* $\wp_\Lambda$*. Hat* $f \in \mathcal{M}(\Lambda)^+$ *Pole nur in* Λ*, so ist* f *sogar ein Polynom in* $\wp_\Lambda$*.*

(3) $\mathcal{M}(\Lambda) = \mathcal{M}(\Lambda)^+(\wp'_\Lambda)$ *ist eine quadratische Körpererweiterung, und es gilt*

$$(\wp'_\Lambda)^2 = 4\,\wp_\Lambda^3 - 60\,G_4(\Lambda)\,\wp_\Lambda - 140\,G_6(\Lambda)\,.$$

Insbesondere ist $\mathcal{M}(\Lambda) = \mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$*.*

Dabei sei für $k \geq 3$ *definiert*

$$G_k(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-k}\,.$$

(Beachte: $G_k(\Lambda) = 0$ *für* k *ungerade.)*

BEWEIS: (1) Siehe oben. Da $\wp$ (modulo Λ) nur einen Pol der Ordnung 2 hat, hat $\wp$ Ordnung 2 als elliptische Funktion. Als Ableitung einer geraden Funktion ist $\wp'$ ungerade. Daß $\wp'$ Ordnung 3 hat, sieht man wie für $\wp$.

(2) Die Hauptteile einer Funktion in $\mathcal{M}(\Lambda)^+$ haben (modulo Λ) die Gestalt

$$\sum_{n=1}^{N} a_n \Big(\frac{1}{(z-w)^n} + \frac{(-1)^n}{(z+w)^n} \Big)\,,$$

falls $2w \notin \Lambda$, bzw.

$$\sum_{n=1}^{N} a_n \frac{1}{(z-w)^{2n}}\,,$$

falls $2w \in \Lambda$ (d.h. $w \equiv -w \bmod \Lambda$). Auf der anderen Seite gilt, daß der einzige Hauptteil mod Λ von $\wp'(w)/(\wp(z) - \wp(w))$ (für $2w \notin \Lambda$) gerade

$$\frac{1}{z-w} - \frac{1}{z+w}$$

ist. Für $2w \in \Lambda$, $w \notin \Lambda$ hat man

$$\frac{1}{(z-w)^2}$$

als Hauptteil von $\wp''(w)/(2(\wp(z) - \wp(w)))$; für $w \in \Lambda$ hat $\wp$ selbst den richtigen Hauptteil. Man sieht, daß man durch eine endliche Linarkombination von Termen $1/(\wp(z) - \wp(w))^n$ bzw. $\wp(z)^n$ eine gerade elliptische Funktion g bekommen kann, die dieselben Hauptteile wie eine gegebene gerade elliptische Funktion f hat. Die Differenz $f - g$ ist dann holomorph, also konstant. Damit ist die erste Aussage bewiesen. Die zweite folgt ebenfalls, da für den Hauptteil bei 0 nur Potenzen von $\wp$ selbst benötigt werden.

(3) Sei $f \in \mathcal{M}(\Lambda)$; dann kann man $f = f_+ + f_-$ schreiben als Summe der geraden Funktion $f_+(z) = (f(z) + f(-z))/2 \in \mathcal{M}(\Lambda)^+$ und der ungeraden Funktion $f_-(z) = (f(z) - f(-z))/2 \in \mathcal{M}(\Lambda)^-$. Da $\wp'$ ungerade ist, ist $f_/\wp'$ gerade. Nach Teil (2) gibt es also rationale Funktionen r_1 und r_2, so daß $f = r_1(\wp) + r_2(\wp)\wp'$

ist. Folglich ist $1, \wp'$ eine Basis von $\mathcal{M}(\Lambda)$ über $\mathcal{M}(\Lambda)^+ = \mathbb{C}(\wp)$, was die erste Aussage beweist.

Da $\wp'$ ungerade ist, ist $(\wp')^2$ gerade; außerdem hat $(\wp')^2$ Pole nur in Λ. Daher muß $(\wp')^2$ ein Polynom in $\wp$ sein. Um die genaue Relation herauszufinden, brauchen wir die Laurentreihe von $\wp$ bei 0.

LEMMA 2.11. *Die Laurentreihe von $\wp_\Lambda(z)$ bei $z = 0$ ist gegeben durch*

$$\wp_\Lambda(z) = z^{-2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2}(\Lambda)\, z^{2n}\,.$$

BEWEIS: Für $|z| < |\omega|$ haben wir

$$(z-\omega)^{-2} - \omega^{-2} = \omega^{-2}\big((1 - z/\omega)^{-2} - 1\big) = \sum_{n=1}^{\infty} (n+1)\omega^{-(n+2)}\, z^n\,.$$

In die definierende Gleichung für $\wp$ eingesetzt und aufsummiert, ergibt das das Ergebnis. (Beachte, daß $G_{2n+1}(\Lambda) = 0$ ist!) □

Die angegebene Gleichung für $(\wp')^2$ ergibt sich nun durch Abgleichen des Hauptteils und des konstanten Terms der Laurentreihe von $(\wp')^2$ wie oben. □

ÜBUNGSAUFGABEN 2.2. Sei Λ ein Gitter, $\wp = \wp_\Lambda$ und $\sigma = \sigma_\Lambda$ usw.

(1) Zeigen Sie, daß für alle $z, w \in \mathbb{C}$ gilt

$$\wp(z) - \wp(w) = -\frac{\sigma(z+w)\sigma(z-w)}{\sigma(z)^2\sigma(w)^2} \quad \text{und} \quad \wp'(z) = \frac{\sigma(2z)}{\sigma(z)^4}\,.$$

(2) Schreiben Sie $\wp''$ und $\wp'''$ als rationalen Ausdruck in $\wp$ und $\wp'$.

(3) Zeigen Sie: Eine auf ganz $\mathbb{C}$ holomorphe Funktion θ mit der Eigenschaft, daß es zu jedem $\omega \in \Lambda$ ein $a_\omega \in \mathbb{C}$ gibt, so daß

$$\theta(z+\omega) = a_\omega\, \theta(z) \quad \text{für alle } z \in \mathbb{C},$$

hat die Form

$$\theta(z) = a\, e^{bz}$$

für geeignete $a, b \in \mathbb{C}$.
Hinweis: Logarithmische Ableitung!

2. Der Satz von Abel-Jacobi

In Satz 2.8 haben wir Einschränkungen an die Null- und Polstellen (mit ihren Vielfachheiten) einer elliptischen Funktion kennengelernt: Die Summe der Null- und Polstellenordnungen (letztere negativ gerechnet), erstreckt über ein Fundamentalparallelogramm, muß verschwinden, und die Summe der Null- und Polstellen selbst (mit den entsprechenden Vielfachheiten) muß in $\mathbb{C}/\Lambda$ ebenfalls verschwinden. In diesem Abschnitt wollen wir nun zeigen, daß das die einzigen Einschränkungen sind. Dazu führen wir eine weitere Funktion ein, die uns als multiplikativer Baustein für elliptische Funktionen dienen kann.

DEFINITION 2.12. Die *Weierstraßsche Sigma-Funktion* (zum Gitter Λ) ist definiert als

$$\sigma(z) = z \prod_{\omega\in\Lambda\setminus\{0\}} \Big(1-\frac{z}{\omega}\Big)\exp\Big(\frac{z}{\omega}+\frac{z^2}{2\omega^2}\Big)\,;$$

ihre logarithmische Ableitung

$$\zeta(z) = \sigma'(z)/\sigma(z) = \frac{1}{z} + \sum_{\omega\in\Lambda\setminus\{0\}} \Big(\frac{1}{z-\omega}+\frac{1}{\omega}+\frac{z}{\omega^2}\Big)$$

heißt *Weierstraßsche Zeta-Funktion*. (Nicht verwechseln mit der *Riemannschen Zeta-Funktion* $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$!)

Hier sind die wichtigsten Eigenschaften.

LEMMA 2.13. *σ ist eine ganze Funktion mit einfachen Nullstellen genau in den Gitterpunkten von Λ. Zu $\omega\in\Lambda$ gibt es Konstanten $a_\omega, b_\omega\in\mathbb{C}$, so daß*

$$\sigma(z+\omega) = e^{a_\omega+b_\omega z}\,\sigma(z)$$

für alle $z\in\mathbb{C}$.

BEWEIS: Es gilt

$$\begin{aligned}\Big(1-\frac{z}{\omega}\Big)\exp\Big(\frac{z}{\omega}+\frac{z^2}{2\omega^2}\Big) &= \Big(1-\frac{z}{\omega}\Big)\Big(1+\frac{z}{\omega}+\frac{z^2}{\omega^2}+O(\omega^{-3})\Big)\\ &= 1+O(\omega^{-3})\,;\end{aligned}$$

also konvergiert das Produkt absolut und gleichmäßig auf kompakten Mengen (die O-Konstante hängt stetig von z ab). Damit ist σ eine ganze Funktion mit Nullstellen genau da, wo einer der Faktoren verschwindet, also genau in den Punkten von Λ.

Für die zweite Aussage beachten wir, daß das Glied in der Reihe für $\zeta(z)$ von der Größenordnung $O(\omega^{-3})$ ist; also konvergiert die Reihe absolut und gleichmäßig in konpakten Teilmengen von $\mathbb{C}\setminus\Lambda$. Wir dürfen also gliedweise differenzieren und sehen, daß $\zeta' = -\wp$ ist. Da $\wp$ elliptisch ist, gibt es also ein $b_\omega\in\mathbb{C}$ mit

$$\zeta(z+\omega) = \zeta(z) + b_\omega \qquad \text{für alle } z\in\mathbb{C}.$$

Wir betrachten jetzt

$$f(z) = \frac{\sigma(z+\omega)}{e^{b_\omega z}\sigma(z)}\,.$$

Es gilt

$$f'(z) = e^{-b_\omega z}(\zeta(z+\omega)-b_\omega\zeta(z))\frac{\sigma(z+\omega)}{\sigma(z)} = 0\,,$$

also ist $f(z) = e^{a_\omega}$ konstant. □

BEMERKUNGEN 2.14.

(1) Die Faktoren $\exp(z/\omega+\frac{1}{2}(z/\omega)^2)$ in der Produktformel für $\sigma(z)$ heißen (aus naheliegenden Gründen) *konvergenzerzeugende Faktoren*. Sie dienen dazu, den Faktor auf die Form $1+O(\omega^{-3})$ zu bringen. Derselbe Trick

funktioniert auch ganz allgemein und liefert den Beweis des *Weierstraßschen Produktsatzes:* Ist in einem Gebiet $D \subset \mathbb{C}$ eine Folge von paarweise verschiedenen Punkten $a_n \in D$ mit Vielfachheiten $v_n \in \mathbb{N}$ gegeben, so daß sich (a_n) nirgends in D häuft, so gibt es eine auf D holomorphe Funktion, deren Nullstellen genau die a_n mit Vielfachheit v_n sind. Als konvergenzerzeugende Faktoren muß man dabei

$$\exp(z/a_n + \tfrac{1}{2}(z/a_n)^2 + \cdots + \tfrac{1}{k_n}(z/a_n)^{k_n})$$

mit geigneten k_n nehmen.

(2) Eine Funktion, die ein Transformationsverhalten wie σ aufweist, heißt auch *Thetafunktion* bezüglich Λ. Wichtig sind besonders ihre Verallgemeinerungen auf Gitter in $\mathbb{C}^n$.

(3) Aus $\sigma(z + (\omega_1 + \omega_2)) = \sigma((z + \omega_1) + \omega_2)$ bekommt man

$$b_{\omega_1+\omega_2} = b_{\omega_1} + b_{\omega_2} \quad \text{und}$$
$$a_{\omega_1+\omega_2} = a_{\omega_1} + b_{\omega_1}\omega_2 + a_{\omega_2} \bmod 2\pi i\mathbb{Z}\,.$$

b definiert also einen Homomrphismus $\Lambda \to \mathbb{C}$, während das Paar (a, b) einen 1-Kozykel (siehe später) $\Lambda \to \mathbb{C}/2\pi i\mathbb{Z} \times \mathbb{C}$ definiert, wobei Λ auf $\mathbb{C}/2\pi i\mathbb{Z} \times \mathbb{C}$ operiert durch $(\alpha, \beta)^\omega = (\alpha + \beta\omega, \beta)$.

Die Sigma-Funktion stellt uns das nötige Material zur Verfügung, um den Satz von Abel-Jacobi zu beweisen.

Satz 2.15 (Abel-Jacobi). *Sei F ein Fundamentalparallelogramm für Λ, und seien $a_1, \ldots, a_n \in F$ paarweise verschieden, $v_1, \ldots, v_n \in \mathbb{Z}$ mit*

$$\sum_{j=1}^{n} v_j = 0 \quad \textit{und} \quad \sum_{j=1}^{n} v_j a_j = \lambda \in \Lambda\,.$$

Dann gibt es $f \in \mathcal{M}(\Lambda)$ mit $\operatorname{ord}_{a_j}(f) = v_j$ für alle j und $\operatorname{ord}_z(f) = 0$ für alle $z \in F \setminus \{a_1, \ldots, a_n\}$.

Beweis: Da σ genau eine einfache Nullstelle modulo Λ hat, liegt folgender Ansatz nahe:

$$f_0(z) = \prod_{j=1}^{n} \sigma(z - a_j)^{v_j}\,.$$

Diese Funktion f_0 hat dann jedenfalls die richtigen Null- und Polstellen. Ist f_0 auch elliptisch? Dazu sei $\omega \in \Lambda$. Es gilt

$$\begin{aligned} f_0(z + \omega) &= \prod_{j=1}^{n} \sigma(z + \omega - a_j)^{v_j} \\ &= \exp(a_\omega \sum_{j=1}^{n} v_j + b_\omega \sum_{j=1}^{n} v_j(z - a_j)) f_0(z) \\ &= \exp(-b_\omega\lambda) f_0(z)\,. \end{aligned}$$

f_0 ist also nur fast elliptisch. Auf der anderen Seite ist aber $\sigma(z)/\sigma(z - \lambda)$ eine ganze Funktion ohne Nullstellen, und es gilt

$$\sigma(z + \omega)/\sigma(z + \omega - \lambda) = \exp(b_\omega\lambda)\sigma(z)/\sigma(z - \lambda)\,;$$

also leistet

$$f(z) = f_0(z)\frac{\sigma(z)}{\sigma(z-\lambda)}$$

das Gewünschte. (Nach Übungsaufgabe 2.2, (3) ist übrigens der Korrekturfaktor $\sigma(z)/\sigma(z-\lambda)$ von der Form ae^{bz}.) □

3. Gitter und Elliptische Kurven

Wir können jetzt die eine Hälfte des Uniformisierungssatzes beweisen.

SATZ 2.16. *Sei $\Lambda \in \mathbb{C}$ ein Gitter und E die durch die affine Gleichung*

$$y^2 = 4\,x^3 - 60G_4(\Lambda)\,x - 140G_6(\Lambda) \tag{3.1}$$

definierte projektive ebene Kurve. Dann ist E eine elliptische Kurve, und die Abbildung

$$\phi : \mathbb{C}/\Lambda \ni z \longmapsto (\wp(z) : \wp'(z) : 1) \in E(\mathbb{C})$$

liefert einen Isomorphismus der Gruppen (und Riemannschen Flächen) $\mathbb{C}/\Lambda$ und $E(\mathbb{C})$.

BEWEIS: Nach Satz 2.10, Teil (3), ist ϕ jedenfalls eine wohldefinierte Abbildung (in der Nähe von 0 muß man die projektiven Koordinaten mit z^3 multiplizieren, um den Pol von $\wp'$ zu eliminieren; dann sieht man, daß $\phi(0) = O$ ist).

Da $\wp$ eine gerade elliptische Funktion der Ordnung 2 ist, sind die Werte

$$e_1 = \wp(\omega_1/2)\,, \quad e_2 = \wp(\omega_2/2)\,, \quad e_3 = \wp((\omega_1+\omega_2)/2)$$

paarweise verschieden (denn $\wp - e_j$ hat eine doppelte Nullstelle). Weiterhin gilt (mit $\omega_3 = \omega_1 + \omega_2$)

$$\wp'(\omega_j/2) = 0 \qquad \text{für } j = 1, 2, 3,$$

da $\wp'$ ungerade ist. Es folgt

$$y^2 = 4(x-e_1)(x-e_2)(x-e_3)\,;$$

also verschwindet die Diskriminante von (3.1) nicht, und es liegt eine elliptische Kurve vor.

Wir zeigen als nächstes, daß ϕ bijektiv ist. Zuerst die Injektivität. Sei $\phi(z_1) = \phi(z_2)$. Wir betrachten $f(z) = \wp(z) - \wp(z_1)$, eine gerade elliptische Funktion der Ordnung 2. Wenn z_1 und z_2 modulo Λ verschieden sind, dann sind z_1 und z_2 genau die beiden einfachen Nullstellen von f. Es folgt $z_2 = -z_1 \pmod{\Lambda}$, also $\wp'(z_2) = -\wp'(z_1)$, und das ist ungleich null, da $2z_1 \equiv z_1 - z_2 \notin \Lambda$. Also $\phi(z_1) \neq \phi(z_2)$, Widerspruch. Daß 0 der einzige Wert mit Bild O ist, ist klar. Zur Surjektivität: Sei $(x, y) \in E(\mathbb{C})$ (O liegt natürlich im Bild). Die Funktion $f(z) = \wp(z) - x$ hat Ordnung 2, also mindestens eine Nullstelle z_0. Wegen Gleichung (3.1) gilt dann $\wp'(z_0) = \pm y$, also $(x, y) = \phi(z_0)$ oder $(x, y) = \phi(-z_0)$.

Es bleibt zu zeigen, daß ϕ auch mit den Gruppenstrukturen verträglich ist. (Die Behauptung, daß ϕ auch ein Isomorphismus Riemannscher Flächen ist, lassen wir außen vor, da wir die nötigen Begriffe nicht eingeführt haben.) Da wir bereits

gesehen haben, daß ϕ bijektiv ist, reicht es aus, zu zeigen, daß für alle Punkte $P_1, P_2, P_3 \in E(\mathbb{C})$ gilt

$$P_1 + P_2 + P_3 = O \quad \Longrightarrow \quad \phi^{-1}(P_1) + \phi^{-1}(P_2) + \phi^{-1}(P_3) = 0\,.$$

Im Fall $P_1 = O$ (z.B.) ist das klar, denn

$$\phi(-z) = (\wp(z), -\wp'(z)) = -(\wp(z), \wp'(z)) = -\phi(z)\,.$$

Seien also o.B.d.A. alle $P_j = (x_j, y_j)$ von O verschieden. Dann liegen sie auf einer Geraden, die nicht parallel zur y-Achse ist:

$$y_j = a\,x_j + b \qquad \text{für } j = 1, 2, 3$$

mit geeigneten $a, b \in \mathbb{C}$. Sei $f(z) = \wp'(z) - a\wp(z) - b$. Dann ist f eine elliptische Funktion der Ordnung 3 (einziger Pol ist bei 0, mit Polordnung 3); ihre drei Nullstellen sind also (mit Vielfachheit) gerade die $\phi^{-1}(P_j)$. Nach Satz 2.8, Teil (3), haben wir also

$$\phi^{-1}(P_1) + \phi^{-1}(P_2) + \phi^{-1}(P_3) - 3 \cdot 0 = 0 \in \mathbb{C}/\Lambda\,;$$

das ist die Behauptung. □

Die andere Hälfte des Uniformisierungssatzes, nämlich daß es zu jeder elliptischen Kurve E über $\mathbb{C}$ ein Gitter Λ gibt, so daß $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ ist wie oben, ist im Grunde auch nicht schwer zu beweisen. Der Beweis erfordert aber einen Einstieg in die Theorie der Modulformen (oder ein genaueres Studium der Integration von Differentialformen auf Riemannschen Flächen), wozu wir hier leider nicht die Zeit haben.

KAPITEL 3

Die Vermutung von Birch und Swinnerton-Dyer

Ich möchte diese etwas isolierte Vorlesung (nachdem fünf Vorlesungen wegen meines Aufenthalts am MSRI ausgefallen waren und dies die letzte Woche vor Weihnachten ist) dazu benutzen, die Vermutung von Birch und Swinnerton-Dyer zu formulieren. Dabei wird sich auch ein Ausblick auf mögliche Themen für den Rest der Vorlesung nach den Weihnachtsferien ergeben.

Sei $E/\mathbb{Q}$ eine elliptische Kurve. Ausgangspunkt für die Vermutung ist der *Satz von Mordell(-Weil)*: Die abelsche Gruppe $E(\mathbb{Q})$ ist *endlich erzeugt.* Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen hat man also eine Zerlegung

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r \,,$$

wobei $E(\mathbb{Q})_{\text{tors}}$ eine endliche abelsche Untergruppe von $E(\mathbb{Q})$ ist, die sogenannte *Torsionsuntergruppe*; und r ist eine natürliche Zahl, der sogenannte *(Mordell-Weil-)Rang* von $E(\mathbb{Q})$.

Der Beweis zerfällt in zwei Schritte. Zuerst zeigt man die notwendige Eigenschaft, daß $E(\mathbb{Q})/2E(\mathbb{Q})$ (oder auch $E(\mathbb{Q})/mE(\mathbb{Q})$ für ein (oder alle) $m \geq 2$) endlich ist. Dann verwendet man die Theorie der *kanonischen Höhe*, um daraus die Behauptung zu folgern.

Was ist nun diese kanonische Höhe? Eine Höhe soll die „Größe“ von Punkten in $E(\mathbb{Q})$ messen. Dazu definiert man erst einmal die *naive Höhe*

$$h(P) = \log \max\{|a|, |b|\} \,, \quad \text{wenn } x(P) = a/b \text{ (gekürzt)}$$

(und $h(O) = 0$). $h(P)$ ist ein Maß dafür, wie viel Platz man braucht, um den Punkt (bzw. seine x-Koordinate) hinzuschreiben. Man kann dann zeigen, daß

$$h(P+Q) + h(P-Q) = 2h(P) + 2h(Q) + O(1)$$

gilt, insbesondere also $(P = Q)$ $h(2P) = 4h(P) + O(1)$. Daraus folgt, daß die kanonische Höhe

$$\hat{h}(P) = \lim_{n\to\infty} 4^{-n} h(2^n P)$$

existiert und folgende Eigenschaften hat.

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q) \quad \text{(Parallelogrammgleichung)}$$

$$\hat{h}(mP) = m^2 \hat{h}(P)$$

$$\hat{h}(P) = 0 \iff P \in E(\mathbb{Q})_{\text{tors}}$$

$$\hat{h}(P) = h(P) + O(1)$$

Aus diesen Eigenschaften folgt auch noch, daß $\hat{h}$ eine positiv definite quadratische Form auf $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$ definiert; die zugehörige Bilinearform ist

$$\langle P, Q \rangle = \tfrac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q))$$

(mit $\langle P, P\rangle = \hat{h}(P)$). Die Gramsche Determinante dieser Form heißt der *(elliptische) Regulator* von E,

$$R(E/\mathbb{Q}) = \det(\langle P_i, P_j\rangle)_{i,j}\,,$$

wobei die P_i eine Basis von $\mathbb{Z}^r \subset E(\mathbb{Q})$ liefern.

Außer $E(\mathbb{Q})_{\text{tors}}$, dem Rang r und dem Regulator $R(E/\mathbb{Q})$ treten in der Vermutung von Birch und Swinnerton-Dyer noch andere Invarianten von E auf. Um sie zu definieren, benötiogt man ein *minimales Weierstraß-Modell* von E. Das ist eine (lange) Weierstraß-Gleichung für E, die ganzzahlige Koeffizienten hat und unter diesen Gleichungen minimalen Betrag der Diskriminante. (Diese Gleichung ist dann auch p-minimal für alle Primzahlen p, d.h., die p-adische Bewertung der Diskriminante ist minimal unter allen ganzzahligen Modellen.)

Mit so einem minimalen Modell definiert man die *reelle Periode* als

$$\Omega(E/\mathbb{Q}) = \int\limits_{E(\mathbb{R})} \Big|\frac{dx}{2y + a_1x + a_3}\Big|\,;$$

dabei muß man den Integrationsweg $E(\mathbb{R})$ (der aus ein oder zwei geschlossenen Kurven besteht) irgendwie orientieren. Die 1-Form $\omega = dx/(2y+a_1x+a_3)$ ist das sogenannte *invariante Differential* von E; sie ist holomorph, hat keine Nullstellen und ist unter Translationen $P \mapsto P + Q$ invariant.

Als nächstes müssen wir die *Tamagawa-Zahlen* definieren. Dazu sei p eine Primzahl. Wir können in einer minimalen Weierstraß-Gleichung für E alle Koeffizienten mod p reduzieren; dann bekommen wir eine Kurve $\tilde{E}$ über $\mathbb{F}_p$. Diese Kurve $\tilde{E}$ kann einen singulären Punkt haben oder aber elliptisch sein. In jedem Fall haben wir eine Reduktionsabbildung

$$E(\mathbb{Q}_p) \ni P \longmapsto \tilde{P} \in \tilde{E}(\mathbb{F}_p)$$

(die kommt durch Einschränkung von $\mathbb{P}^2(\mathbb{Q}_p) \to \mathbb{P}^2(\mathbb{F}_p)$ — wähle projektive Koordinaten in $\mathbb{Z}_p$, die nicht alle durch p teilbar sind, dann bekommt man einen wohldefinierten Punkt mod p). Wir können also definieren

$$E^0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid \tilde{P} \text{ nicht singulär}\}$$
$$E^1(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid \tilde{P} = \tilde{O}\}$$

Es gilt dann, daß $E_1(\mathbb{Q}_p) \subset E^0(\mathbb{Q}_p) \subset E(\mathbb{Q}_p)$ Untergruppen sind. Die Tamagwa-Zahl ist dann gegeben als

$$c_p(E/\mathbb{Q}) = (E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)) = \#E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p)\,.$$

Wenn $\tilde{E}$ eine elliptische Kurve ist (das ist genau dann der Fall, wenn $p \nmid \Delta_E$, also für fast alle p), dann ist natürlich $E^0(\mathbb{Q}_p) = E(\mathbb{Q}_p)$, also $c_p(E/\mathbb{Q}) = 1$. Das Produkt über alle $c_p(E/\mathbb{Q})$ ist also wohldefiniert.

Das letzte und wohl komplizierteste Objekt, das auf der rechten Seite der vermuteten Gleichheit auftritt, ist die *Shafarevich-Tate-Gruppe* $Ш(E/\mathbb{Q})$. Sie besteht aus Isomorphieklassen gewisser *prinzipal homogener Räume* für E. So ein prinzipal homogener Raum (PHR) ist eine Kurve X über $\mathbb{Q}$ vom Geschlecht 1, auf der E durch Translation einfach transitiv operiert, d.h. man hat einen über $\mathbb{Q}$ definierten Morphismus $\phi_X : E \times X \to X$, $(P, Q) \mapsto P + Q$, der die üblichen Axiome einer Gruppenoperation erfüllt, und wenn ich einen Punkt $Q_0 \in X(\bar{\mathbb{Q}})$

wähle, dann bekomme ich einen über $\bar{\mathbb{Q}}$ definierten Isomorphismus $P \mapsto P + Q_0$ von E und X. Zwei solche PHR X und X' für E heißen *isomorph*, wenn es einen (über $\mathbb{Q}$ definierten) Isomorphismus $\varphi : X \to X'$ gibt, so daß $\varphi \circ \phi_X = \phi_{X'} \circ (\mathrm{id}_E \times \varphi)$ gilt. Die Menge der Isomorphieklassen von PHR für E trägt eine Struktur als abelsche Gruppe; sie kommt von der *Baer-Summe*: Zu zwei PHR X und Y bildet man den PHR $Z = X \times Y/\sim$, wobei $\sim$ gegeben ist durch $(P + Q, R) \sim (Q, P + R)$ für alle $P \in E$, $Q \in X$, $R \in Y$. Die Operation ϕ_Z ist gegeben durch $P + [(Q, R)] = [(P + Q, R)] = [(Q, P + R)]$ (wobei $[(Q, R)]$ die Äquivalenzklasse von (Q, R) bezeichnet). Das neutrale Element dieser Gruppe ist die Isomorphieklasse der *trivialen* PHR; sie sind isomorph zu E, operierend auf sich selbst durch Translation. Ein PHR X ist genau dann trivial, wenn er einen rationalen Punkt hat, denn mit diesem Punkt als Basispunkt bekommen wir einen über $\mathbb{Q}$ definierten Isomorphismus von E und X. Das Negative zu einem PHR X ist gegeben durch X mit der Operation $(P, Q) \mapsto -P + Q$; die Diagonale $\{(Q, Q) \mid Q \in X\} \subset X \times X$ bildet eine Äquivalenzklasse, die einen rationalen Punkt auf der Baer-Summe liefert. Die Gruppe aller Isomorphieklassen von PHR für E heißt die *Weil-Chatelet-Gruppe* von E.

In der Weil-Chatelet-Gruppe gibt es die Untergruppe der *lokal trivialen* PHR. Das sind diejenigen PHR X, für die gilt $X(\mathbb{Q}_p) \neq \emptyset$ für alle Primzahlen p und $X(\mathbb{R}) \neq \emptyset$. Sie besitzen also reelle Punkte und Punkte „modulo n“ für alle natürlichen Zahlen n. Im Unterschied zu Kurven vom Geschlecht 0 folgt daraus aber nicht, daß X auch einen rationalen Punkt hat, also trivial ist. Diese Untergruppe, und das ist die Shafarevich-Tate-Gruppe $Ш(E/\mathbb{Q})$, mißt also, in welchem Ausmaß dieses sogenannte *Hasse-Prinzip* für die PHR für E schief geht. Es wird vermutet, daß diese Gruppe stets endlich ist; bewiesen ist das jedoch nur in einigen Spezialfällen (siehe unten).

Nun haben wir alle Invarianten kennengelernt, die auf der rechten Seite der Vermutung von Birch und Swinnerton-Dyer auftreten. Auf der linken Seite steht die *L-Reihe* von E. Sie wird gebildet aus Information über das Verhalten von E bei Reduktion mod p, für alle Primzahlen p. Dazu müssen wir genauer betrachten, was bei dieser Reduktion passieren kann. Sei E gegeben durch eine minimale Weierstraß-Gleichung und p eine Primzahl. Wir erhalten eine Kurve $\tilde{E}$ über $\mathbb{F}_p$, indem wir die Koeffizienten mod p reduzieren. Es können nun 3 Fälle auftreten.

1. $\tilde{E}$ ist eine elliptische Kurve. Man spricht dann von *guter Reduktion* bei p. Das ist der Fall, wenn p die Diskriminante Δ_E nicht teilt. In diesem Fall setzen wir $\varepsilon(p) = 1$ und $a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p)$.
2. $\tilde{E}$ hat einen einfachen Doppelpunkt als Singularität. Für $p \neq 2$ kann die Gleichung mod p dann in die Form $y^2 = x^2(x - a)$ gebracht werden (mit $a \in \mathbb{F}_p^\times$). Man spricht von *multiplikativer Reduktion* bei p. (Die nicht-singulären Punkte von $\tilde{E}$ bilden unter der üblichen Vorschrift eine Gruppe, die (über $\bar{\mathbb{F}}_p$) zur multiplikativen Gruppe isomorph ist.) Wir setzen $\varepsilon(p) = 0$ und $a_p = -1$ bzw. $a_p = 1$, wenn die Steigungen der beiden Tangenten in $\mathbb{F}_p$ liegen (d.h. a ist ein Quadrat) bzw. wenn die Tangentensteigungen in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ liegen (d.h. a ist kein Quadrat).
3. $\tilde{E}$ hat eine Spitze (Kuspe) als Singularität. Die Gleichung von $\tilde{E}$ sieht dann aus wie $y^2 = x^3$. Man spricht von *additiver Reduktion* bei p. (In

diesem Fall ist die Gruppe der nicht-singulären Punkte isomorph (bereits über $\mathbb{F}_p$) zur additiven Gruppe.) Wir setzen $\varepsilon(p) = 0$ und $a_p = 0$.

Mit diesen Bezeichungen ist die L-Reihe definiert als

$$L(E,s) = \prod_p \frac{1}{1 - a_p\, p^{-s} + \varepsilon(p)\, p^{1-2s}} = \sum_{n=1}^{\infty} a_n\, n^{-s}\,.$$

(Die Koeffizienten a_n bekommt man durch formales Ausmultiplizieren der geomoetrischen Reihen $\sum_{k=0}^{\infty}(a_p p^{-s} - \varepsilon(p)p^{1-2s})^k$. Insbesondere ist die L-Reihe eine Dirichlet-Reihe.) Das Produkt konvergiert jedenfalls für $\mathrm{Re}(s) > 3/2$; das liegt daran, daß $|a_p| \le 2\sqrt{p}$ ist. Aus dem Beweis der Modularitätsvermutung für elliptische Kurven über $\mathbb{Q}$ durch Wiles und andere folgt, daß $L(E,s)$ eine holomorphe Fortsetzung auf ganz $\mathbb{C}$ hat und einer Funktionalgleichung genügt: Sei

$$\Lambda(E,s) = N^{-s/2}(2\pi)^{-s}\Gamma(s)L(E,s)\,;$$

dann gilt

$$\Lambda(E, 2-s) = \pm\Lambda(E,s)$$

mit einem nur von E abhängigen Vorzeichen. N ist dabei eine natürliche Zahl, der sogenannte *Führer* von E. Es gilt $N = \prod_p p^{n_p}$ mit $n_p = 0$ bei guter Reduktion, $n_p = 1$ bei multiplikativer Reduktion und $n_p \ge 2$ bei additiver Reduktion (wobei für $p \ge 5$ in diesem Fall $n_p = 2$ gilt).

Jetzt haben wir (endlich!) alles beisammen, um die Vermutung von Birch und Swinnerton-Dyer hinschreiben zu können.

Vermutung (Birch und Swinnerton-Dyer):

(1) $\mathrm{ord}_{s=1} L(E,s) = r$;
(2) $Ш(E/\mathbb{Q})$ ist endlich;
(3)

$$L(E, 1+t) = \frac{R(E/\mathbb{Q})\Omega(E/\mathbb{Q})\prod_p c_p(E/\mathbb{Q})\#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2}\, t^r + O(t^{r+1})\,.$$

Zur Erinnerung: r ist der Mordell-Weil-Rang von $E(\mathbb{Q})$. Die erste Aussage behauptet also, daß die Verschwindungsordnung von $L(E,s)$ bei $s=1$ gleich dem Rang von E sei. Die zweite Behauptung ist notwendig, um die dritte formulieren zu können, die eine genaue Aussage macht über den führenden Koeffizienten der Taylor-Entwicklung von $L(E,s)$ bei $s=1$.

Diese Vermutung ist insofern erstaunlich, als sie einen überraschenden Zusammenhang zwischen Information mod p (auf der linken Seite) und „globalen“ (also von E über $\mathbb{Q}$ abhängigen) Invarianten wie r, $R(E/\mathbb{Q})$ und $Ш(E/\mathbb{Q})$ herstellt. Es gibt hier eine gewisse Analogie mit der *analytischen Klassenzahlformel*, die einen ähnlichen Zusammenhang liefert zwischen dem Residuum der Dedekindschen Zetafunktion eines Zahlkörpers und seinem Regulator und seiner Klassenzahl. Tatsächlich sind beide Aussagen Spezialfälle von sehr allgemeinen Vermutungen über „spezielle Werte von L-Reihen“.

Was ist nun über diese Vermutung bekannt? Lange Zeit so gut wie gar nichts, doch inzwischen gibt es einige Resultate: Wenn der *analytische Rang* $\mathrm{ord}_{s=1} L(E,s)$ höchstens 1 ist, dann sind (1) und (2) richtig, und (3) stimmt bis auf einen

beschränkten rationalen Faktor. Wenn die elliptische Kurve komplexe Multiplikation hat, dann gelten (1) und (2) auch, wenn $r \leq 1$ ist, und der eventuelle Korrekturfaktor in (3) ist noch weiter eingeschränkt. Für allgemeine Kurven ist jedoch nicht gezeigt, daß aus $r \leq 1$ folgt, daß der analytische Rang ebenfalls ≤ 1 ist. Und für Ränge ≥ 2 ist so gut wie nichts bekannt.

KAPITEL 4

Der Satz von Mordell-Weil

1. Einführung

In diesem letzten Teil der Vorlesung wollen wir den Satz von Mordell-Weil beweisen. Er sagt folgendes aus.

SATZ 4.1 (Mordell-Weil). *Sei K ein algebraischer Zahlkörper und E/K eine elliptische Kurve. Dann ist die abelsche Gruppe $E(K)$ der K-rationalen Punkte auf E endlich erzeugt.*

Der Beweis dieses Satzes zerfällt in zwei recht verschiedene Teile. Zunächst zeigt man, daß folgende notwendige Bedingung erfüllt ist.

SATZ 4.2 (schwacher Satz von Mordell-Weil). *Für ein (oder alle) $m \geq 2$ ist $E(K)/mE(K)$ endlich.*

Wenn man die Grundresultate der algebraischen Zahlentheorie voraussetzt, nämlich Endlichkeit der Klassenzahl und endliche Erzeugtheit der Einheitengruppe, dann gibt es für den Fall $m = 2$ einen ziemlich elementaren Beweis; siehe z.B. [Cas, § 15]. Da der Hintergrund aber „eigentlich“ die Galoiskohomologie von E ist, möchte ich dafür etwas weiter ausholen und eine kurze Einführung in diese Theorie geben. Zunächst möchte ich aber die Skizze der Beweisstrategie vervollständigen. Die Aussage des schwachen Satzes von Mordell-Weil ist nicht hinreichend für die endliche Erzeugtheit von $E(K)$, wie die additiven Gruppen $\mathbb{Q}$ oder $\mathbb{R}$ zeigen. Das Problem bei diesen Beispielen ist, daß sich Gruppenelemente beliebig oft durch m teilen lassen. Der zweite Teil des Beweises zeigt, daß dies bei $E(K)$ nicht passieren kann.

PROPOSITION 4.3. *Es gibt eine* Höhenfunktion $h : E(K) \to \mathbb{R}_{\geq 0}$ *mit folgenden Eigenschaften.*

(i) *Für jedes C ist die Menge $\{P \in E(K) \mid h(P) \leq C\}$ endlich.*
(ii) *Für jeden Punkt $Q \in E(K)$ gibt es eine Konstante $c(Q)$, so daß für alle $P \in E(K)$ gilt:*

$$h(P+Q) \leq 2\,h(P) + c(Q)\,.$$

(iii) *Für ein $m \geq 2$, für das der schwache Satz von Mordell-Weil gilt, gibt es eine Konstante c_m, so daß für alle $P \in E(K)$ gilt:*

$$h(mP) \geq m^2\,h(P) - c_m\,.$$

Aus beiden Teilaussagen folgt nun der Satz in der folgenden Weise.

KOROLLAR 4.4. *Sei $m \geq 2$ wie oben. Seien $Q_i \in E(K)$ $(i = 1, \ldots, k)$ Repräsentanten der Restklassen in $E(K)/mE(K)$ (das sind endlich viele nach Teil 1), und sei*

$$\gamma = \frac{1}{m^2 - 2}(c_m + \max\{c(-Q_i) \mid i = 1, \ldots, k\}) .$$

Dann wird $E(K)$ von der endlichen Menge

$$M = \{Q_i \mid i = 1, \ldots, k\} \cup \{P \in E(K) \mid h(P) \leq \gamma\}$$

erzeugt.

BEWEIS: Sei $c' = \max\{c(-Q_i) \mid i = 1, \ldots, k\}$. Die Menge M ist endlich nach Eigenschaft (i) von h. Wir nehmen nun an, die Aussage sei falsch. Dann gibt es (wiederum wegen Eigenschaft (i)) einen Punkt $P \in E(K)$ minimaler Höhe $h(P)$ mit $P \notin \langle M \rangle$. Offenbar ist dann $h(P) > \gamma$. Nun gibt es genau ein i, so daß wir schreiben können $P = Q_i + mP'$ mit einem $P' \in E(K)$. Aus den Eigenschaften (ii) und (iii) von h bekommen wir dann

$$2\,h(P) + c' \geq h(P - Q_i) = h(mP') \geq m^2\,h(P') - c_m\,,$$

also

$$h(P') \leq \frac{2}{m^2}\,h(P) + \frac{c_m + c'}{m^2} = \frac{2}{m^2}\,h(P) + \left(1 - \frac{2}{m^2}\right)\gamma < h(P)$$

(da $h(P) > \gamma$). Nach Wahl von P ist $P' \in \langle M \rangle$, also liegt auch $P = Q_i + mP'$ in der von M erzeugten Untergruppe, Widerspruch. □

Zum Abschluß dieser Einführung noch ein paar Bemerkungen zur Effektivität dieser Aussage. Der zweite Teil ist effektiv, d.h. man kann bei gegebener Kurve E, gegebenem m und gegebenem $Q \in E(K)$ geeignete Konstanten c_m und $c(Q)$ explizit berechnen. Auch Eigenschaft (i) ist effektiv — man kann die angegebene endliche Menge aufzählen.

Der erste Teil ist problematischer. Um ein endliches Erzeugendensystem von $E(K)$ angeben zu können, braucht man explizite Erzeuger von $E(K)/mE(K)$. Bis heute kann man jedoch nicht beweisen, daß es einen Algorithmus gibt, der solche immer liefert. (Wenn man die Vermutung, daß $Ш(E/K)$ endlich ist, akzeptiert, dann gibt es einen Algorithmus; aber diese Vermutung ist völlig offen. Wir werden den Zusammenhang später sehen.) Was man in der Praxis tun kann, ist, für kleines m ($m = 2$, 3, 4, in Ausnahmefällen auch etwas größere kleine Primzahlen) die Ordnung der Gruppe $E(K)/mE(K)$ nach oben zu beschränken. Wenn man dann ebenso viele Restklassen findet, hat man diese Gruppe bestimmt, aber es gibt keine Garantie dafür, daß die Schranke für $\#(E(K)/mE(K))$ scharf ist. (Das Hindernis kommt von der m-Torsion $Ш(E/K)[m]$.)

2. Gruppenkohomologie (Schmalspurversion)

Literatur: [Si1, Appendix B] oder (als richtige Einführung in die Gruppenkohomologie mit allem Drum und Dran) [Bro].

„Schmalspurversion“ deshalb, weil ich mich auf die Definition von H^0 und H^1 und ihre wichtigsten Eigenschaften beschränken werde. Man kann jedoch (siehe [Bro]) Kohomologiegruppen H^j für alle $j \geq 0$ definieren. Vor allem einige

H^2-Gruppen spielen in der Zahlentheorie durchaus eine Rolle (Stichwort *Brauergruppe*).

Ausgangspunkt für die Gruppenkohomologie ist ein G-Rechtsmodul M, also eine abelsche Gruppe M, auf der die (nicht notwendig abelsche) Gruppe G von rechts durch Automorphismen operiert. Wir werden die Operation in Exponentialschreibweise $M \times G \ni (m, \sigma) \mapsto m^\sigma \in M$ notieren. So ein Modul hat eine ausgezeichnete Untergruppe:

DEFINITION 4.5. Die Untergruppe der *G-Invarianten* von M ist

$$M^G = \{m \in M \mid m^\sigma = m \text{ für alle } \sigma \in G\}\,.$$

Zur Motivation der Einführung der Kohomologiegruppen betrachten wir eine kurze exakte Sequenz von G-Moduln (d.h. die Abbildungen sind G-Homomorphismen — Homomorphismen von abelschen Gruppen, die mit der G-Operation verträglich sind: $\phi(m^\sigma) = \phi(m)^\sigma$):

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0\,.$$

Man überlegt sich leicht (siehe auch unten), daß man für die G-Invarianten folgende exakte Sequenz bekommt:

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G\,.$$

Die letzte Abbildung muß aber nicht surjektiv sein. (Als Beispiel betrachte man $A = 2\mathbb{Z}/4\mathbb{Z}$, $B = \mathbb{Z}/4\mathbb{Z}$, $C = \mathbb{Z}/2\mathbb{Z}$ und $G = \{\pm 1\}$, operierend durch Multiplikation.) In kategorientheoretischer Sprache würde man sagen: Der Funktor $M \mapsto M^G$ ist (nur) linksexakt. Das wirft die Frage auf, wie man das Schiefgehen der Exaktheit auf der rechten Seite messen kann. Hier kommt nun die Kohomologie ins Spiel.

DEFINITION 4.6. Sei G eine Gruppe und M ein G-Rechtsmodul.

(1) $H^0(G, M) = M^G$.
(2) $Z^1(G, M) = \{\xi : G \to M \mid \forall \sigma, \tau \in G : \xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau\}$
(Gruppe der *1-Kozykel* von G nach M).
$B^1(G, M) = \{\sigma \mapsto m^\sigma - m \mid m \in M\} \subset Z^1(G, M)$
(Gruppe der *1-Koränder* von G nach M).
$H^1(G, M) = Z^1(G, M)/B^1(G, M)$
(*Erste Kohomologiegruppe* von G mit Werten in M).

Als einfaches Beispiel betrachten wir den Fall, daß die Operation von G auf M trivial ist, d.h. $m^\sigma = m$ für alle $m \in M$, $\sigma \in G$. Dann gilt offenbar

$$H^0(G, M) = M \qquad \text{und} \qquad H^1(G, M) = \mathrm{Hom}(G, M)\,,$$

denn die *Kozykelbedingung* $\xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau$ wird im Fall der trivialen Operation gerade zu der Bedingung für einen Homomorphismus, und alle Koränder sind 0.

Im allgemeinen kann man sich ein Element der Kohomologiegruppe $H^1(G, M)$ durch einen Kozykel repräsentiert denken; man muß nur beachten, daß zwei Kozykel dieselbe Kohomologieklasse definieren, wenn sie sich um einen Korand unterscheiden.

Die erste wichtige Eigenschaft der Kohomologiegruppen ist, daß sie tatsächlich die Abweichung von der Rechtsexaktheit messen.

PROPOSITION 4.7 (Lange exakte Kohomologiesequenz).
Sei $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ *eine kurze exakte Sequenz von G-Moduln. Dann hat man eine exakte Sequenz*

$$\begin{aligned} 0 \longrightarrow H^0(G,A) &\xrightarrow{\alpha_*} H^0(G,B) \xrightarrow{\beta_*} H^0(G,C) \\ &\xrightarrow{\delta} H^1(G,A) \xrightarrow{\alpha_*} H^1(G,B) \xrightarrow{\beta_*} H^1(G,C)\,. \end{aligned}$$

Der sogenannte verbindende Homomorphismus δ *ist dabei wie folgt definiert. Sei* $c \in C^G = H^0(G,C)$*. Dann gibt es* $b \in B$ *mit* $\beta(b) = c$*. Wir bilden den Korand* $(\xi_\sigma = b^\sigma - b) \in B^1(G,B)$*. Da* $\beta(b) = c = c^\sigma = \beta(b^\sigma)$*, liegt* ξ_σ *im Kern von* β*, also gibt es* $a_\sigma \in A$ *mit* $\alpha(a_\sigma) = \xi_\sigma$*. Das definiert einen Kozykel* $a \in Z^1(G,A)$*; seine Klasse in* $H^1(G,A)$ *ist* $\delta(c)$*.*

BEWEIS: Zuerst ist zu zeigen, daß δ wohldefiniert ist, d.h., daß $\delta(c)$ nicht von der Wahl von $b \in B$ mit $\beta(b) = c$ abhängt. Sei also $b' \in B$ mit $\beta(b') = c$ und ξ', a' die mit b' gebildeten Kozykel. Da $\beta(b'-b) = c - c = 0$, gibt es ein $z \in A$ mit $\alpha(z) = b' - b$. Es folgt, daß $a'_\sigma = a_\sigma + (z^\sigma - z)$, also unterscheiden sich a und a' um einen Korand und repräsentieren deshalb dieselbe Klasse in $H^1(G,A)$.

Nun zur Exaktheit. Die Injektivität von α_* auf H^0 ist klar, denn dies ist die Einschränkung des injektiven Homomorphismus α auf $A^G \subset A$. Zur Exaktheit bei $H^0(G,B)$: $\beta_*\alpha_* = 0$ ist klar. Sei $b \in B^G$ im Kern von β_*; dann gibt es jedenfalls $a \in A$ mit $\alpha(a) = b$, und a ist eindeutig bestimmt. Da $\alpha(a^\sigma) = \alpha(a)^\sigma = b^\sigma = b$ ist für alle $\sigma \in G$, muß $a = a^\sigma$, also $a \in A^G$ sein.

Für die Exaktheit bei $H^0(G,C)$ ist zunächst $\delta\beta_* = 0$ zu zeigen. Sei also $b \in B^G$ und $c = \beta(b)$. Dann können wir dieses b verwenden, um $\delta(c)$ zu berechnen. Da b invariant ist, ist dann aber bereits $\xi = 0$, also erst recht $\delta(c) = 0$. Sei nun $c \in C^G$ mit $\delta(c) = 0$. Das bedeutet, daß der Kozykel a ein Korand ist: $a_\sigma = z^\sigma - z$ für ein $z \in A$. Indem wir b ersetzen durch $b - \alpha(z)$, können wir annehmen, daß bereits $\xi = 0$ ist. Das bedeutet aber gerade, daß $b \in B^G$ ist, und damit ist $c = \beta(b)$ im Bild von β_*.

Exaktheit bei $H^1(G,A)$: Zunächst zeigen wir $\alpha_*\delta = 0$. Seien also $c \in C^G$ und b, ξ, a wie in der Definition von $\delta(c)$. Dann ist $\alpha_*(\delta(c))$ nach Definition von δ gerade die Klasse des Kozykels $\xi \in Z^1(G,B)$; ξ ist aber nach Konstruktion ein Korand, also ist $\alpha_*(\delta(c)) = 0$. Sei nun $a \in Z^1(G,A)$ ein Kozykel, dessen Bild in $Z^1(G,B)$ ein Korand ist: $\alpha(a_\sigma) = b^\sigma - b$. Dann ist $c = \beta(b)$ invariant (wegen $\beta\alpha = 0$), und nach Konstruktion ist $a = \delta(c)$ im Bild von δ.

Zur Exaktheit bei $H^1(G,B)$: $\beta_*\alpha_* = 0$ ist klar. Sei nun also $b \in Z^1(G,B)$ ein Kozykel, dessen Bild in $Z^1(G,C)$ ein Korand ist: $\beta(b_\sigma) = c^\sigma - c$. Da β surjektiv ist, gibt es ein $y \in B$ mit $\beta(y) = c$. Indem wir b_σ durch $b_\sigma - (y^\sigma - y)$ ersetzen, können wir annehmen, daß $\beta(b_\sigma) = 0$ ist. Dann gibt es aber eindeutig bestimmte $a_\sigma \in A$ mit $\alpha(a_\sigma) = b_\sigma$; es ist leicht zu sehen, daß die so definierte Abbildung $a : G \to A$ ein Kozykel ist. Damit ist gezeigt, daß die Kohomologieklasse von b im Bild von α_* liegt. □

BEMERKUNG 4.8. Wenn man die höheren Kohomologiegruppen H^2, H^3 etc. definiert hat, dann kann man die lange exakte Kohomologiesequenz entsprechend fortsetzen (mit verbindenden Homomorphismen $H^j(G,C) \to H^{j+1}(G,A)$).

Für die Anwendung am wichtigsten ist der Fall, daß G eine endliche Gruppe ist. In diesem Fall hat man eine recht starke Aussage über die Struktur von $H^1(G,M)$.

PROPOSITION 4.9. *Ist G eine endliche Gruppe der Ordnung n, dann annulliert n die Kohomologiegruppe $H^1(G,M)$ für jeden G-Modul M.*

BEWEIS: Sei $\xi \in Z^1(G,M)$ ein Kozykel. Wir müssen zeigen, daß $n\xi$ ein Korand ist. Dafür ist ein Element $m \in M$ zu finden mit $m^\sigma - m = n\,\xi_\sigma$ für alle $\sigma \in G$. Das einzige Element, das einem in dieser allgemeinen Situation in den Sinn kommt, ist $m = \sum_{\sigma\in G} \xi_\sigma$. Mit diesem m gilt dann

$$m^\tau = \sum_\sigma \xi_\sigma^\tau = \sum_\sigma (\xi_{\sigma\tau} - \xi_\tau) = m - n\,\xi_\tau\,,$$

also ist $n\,\xi_\tau = (-m)^\tau - (-m)$ tatsächlich ein Korand. □

Insbesondere gilt für die triviale Gruppe $G = \{1\}$ stets $H^1(\{1\},M) = 0$. Ebenso gilt für einen Modul M, der von einer natürlichen Zahl k mit $\mathrm{ggT}(\#G,k) = 1$ annulliert wird, daß $H^1(G,M) = 0$ ist.

Im speziellen Fall, daß G endlich zyklisch ist, gibt es eine relativ einfache „Formel“ für $H^1(G,M)$.

PROPOSITION 4.10. *Sei G zyklisch der Ordnung n mit Erzeuger σ. Dann gilt*

$$H^1(G,M) \cong \frac{\{m \in M \mid \sum_{j=0}^{n-1} m^{\sigma^j} = 0\}}{\{m^\sigma - m \mid m \in M\}}\,.$$

BEWEIS: Aus der Kozykelrelation folgt für jedes $\xi \in Z^1(G,M)$, daß

$$\xi_{\sigma^j} = \xi_\sigma + \xi_\sigma^\sigma + \cdots + \xi_\sigma^{\sigma^{j-1}}\,. \tag{2.1}$$

Die Abbildung $Z^1(G,M) \ni \xi \mapsto \xi_\sigma \in M$ ist also injektiv. Was ist ihr Bild? Die Relation $0 = \xi_1 = \xi_{\sigma^n}$ zeigt, daß das Bild enthalten ist in $M_1 = \{m \in M \mid \sum_{j=0}^{n-1} m^{\sigma^j} = 0\}$. Umgekehrt kann man leicht nachprüfen, daß für $m \in M_1$ die Abbildung ξ mit $\xi_\sigma = m$ und sonst definiert wie in (2.1) tatsächlich ein Kozykel ist. Das Bild der Koränder ist offensichtlich $M_2 = \{m^\sigma - m \mid m \in M\}$, also ist $H^1(G,M) \cong M_1/M_2$ wie behauptet. □

Das letzte grundlegende Resultat in diesem Abschnitt beschäftigt sich damit, was passiert, wenn man die Gruppe wechselt. Zunächst einmal betrachten wir die Situation, daß wir eine Untergruppe $H \subset G$ haben. Jeder G-Modul ist dann automatisch auch ein H-Modul, indem man die G-Operation $M \times G \to M$ auf $M \times H$ einschränkt. Entsprechend kann man Kozykel $G \to M$ auf H einschränken, und da offensichtlich Koränder nach Einschränkung immer noch Koränder sind, bekommen wir eine *Restriktionsabbildung*

$$\mathrm{res} : H^1(G,M) \longrightarrow H^1(H,M) \quad \text{und ebenso} \quad H^0(G,M) \longrightarrow H^0(H,M)\,;$$

letztere ist eine Inklusion (ein G-invariantes Element ist erst recht H-invariant).

Wenn nun H sogar ein Normalteiler ist, dann wird M^H auf natürliche Weise ein $H\backslash G$-Rechtsmodul — wir definieren

$$m^{H\sigma} = m^\sigma\,;$$

die Wahl des Repräsentanten $\sigma \in G$ spielt keine Rolle, da mit $\tau \in H$ wegen $m \in M^H$ gilt: $m^{\tau\sigma} = m^\sigma$. Wenn wir einen Kozykel $\xi \in Z^1(H\backslash G, M^H)$ haben, dann können wir ihn zurückziehen zu einer Abbildung

$$\Xi : G \longrightarrow H\backslash G \longrightarrow M^H \longrightarrow M\,,$$

und es ist leicht zu sehen, daß Ξ wieder ein Kozykel ist, und daß Koränder auf Koränder abgebildet werden. Das liefert die *Inflationsabbildung*

$$\inf : H^1(H\backslash G, M^H) \longrightarrow H^1(G, M) \quad \text{und auch} \quad H^0(H\backslash G, M^H) \longrightarrow H^0(G, M)\,;$$

letztere ist sogar ein Isomorphismus.

Nun haben wir folgendes wichtiges Resultat, das diese beiden Abbildungen miteinander verknüpft.

Proposition 4.11 (Inflations-Restriktions-Sequenz). *Sei G eine Gruppe und $H \subset G$ ein Normalteiler, sowie M ein G-Modul. Dann ist folgende Sequenz exakt.*

$$0 \longrightarrow H^1(H\backslash G, M^H) \xrightarrow{\inf} H^1(G, M) \xrightarrow{\text{res}} H^1(H, M)\,.$$

Beweis: Exaktheit bei $H^1(H\backslash G, M^H)$: Sei $\xi \in Z^1(H\backslash G, M^H)$ mit $\inf(\xi) \in B^1(G, M)$. Es gibt also $m \in M$, so daß für alle $\tau \in H$, $\sigma \in G$ gilt:

$$m^\sigma - m = \inf(\xi)_\sigma = \xi_{H\sigma} = \inf(\xi)_{\tau\sigma} = m^{\tau\sigma} - m\,.$$

Wenn wir $\sigma = 1$ wählen, sehen wir, daß $m \in M^H$ sein muß. Dann folgt aber auch, daß ξ der von $m \in M^H$ erzeugte Korand ist.

Exaktheit bei $H^1(G, M)$: Wir zeigen erst einmal $\operatorname{res}\inf = 0$. Sei dazu wieder $\xi \in Z^1(H\backslash G, M^H)$. Für $\tau \in H$ ist dann

$$\operatorname{res}(\inf(\xi))_\tau = \inf(\xi)_\tau = \xi_{H\tau} = \xi_H = 0\,,$$

also $\operatorname{res}(\inf(\xi)) = 0$ sogar als Kozykel. Sei nun $\Xi \in Z^1(G, M)$ mit $\operatorname{res}(\Xi) \in B^1(G, H)$. Es gibt also $m \in M$ mit $\Xi_\tau = m^\tau - m$ für alle $\tau \in H$. Indem wir den von m erzeugten Korand von Ξ subtrahieren, können wir annehmen, daß $\Xi_\tau = 0$ ist für alle $\tau \in H$. Aus der Kozykelrelation folgt nun für alle $\tau \in H$ und $\sigma \in G$, daß

$$\Xi_{\tau\sigma} = \Xi_\tau^\sigma + \Xi_\sigma = \Xi_\sigma$$

und außerdem, daß

$$\Xi_\sigma^\tau = \Xi_{\sigma\tau} - \Xi_\tau = \Xi_{\sigma\tau} = \Xi_{\tau'\sigma} = \Xi_\sigma$$

ist (wobei $\tau' \in H$ mit $\sigma\tau = \tau'\sigma$ ist; das ist möglich, da H Normalteiler ist). Beide Aussagen zusammen zeigen, daß Ξ faktorisiert als

$$G \longrightarrow H\backslash G \xrightarrow{\xi} M^H \longrightarrow M\,,$$

also ist $\Xi = \inf(\xi)$. □

Die Wichtigkeit dieses Ergebnisses liegt darin, daß man die Berechnung der Kohomologie zurückführen kann auf die Berechnung der Kohomologie von kleineren Gruppen. Wir werden im Folgenden der Einfachheit halber G/H statt $H\backslash G$ schreiben; wenn man mit Kozykeln etc. tatsächlich rechnen will, muß man aber beachten, daß der Quotient als Menge der Rechtsnebenklassen $H\sigma$ zu interpretieren ist.

3. Galoiskohomologie

3.1. Projektive und injektive Limites. Pro-endliche Gruppen. Wir werden die folgenden Konstruktionen für Gruppen durchführen; sie sind aber genauso möglich für Ringe, Moduln, ... Literatur hierfür ist zum Beispiel Gruenbergs Chapter V in [CF].

Als motivierendes Beispiel betrachten wir die absolute Galoisgruppe $\mathrm{Gal}_K = \mathrm{Gal}(\bar{K}/K)$ eines Zahlkörpers K. Der algebraische Abschluß $\bar{K}$ ist die Vereinigung (ein spezieller injektiver Limes!) der endlichen Galoiserweiterungen L/K mit $L \subset \bar{K}$. Das liefert uns ein System von (endlichen) Gruppen $G_L = \mathrm{Gal}(L/K)$, zusammen mit Homomorphismen $\phi_{L,M} : G_M \to G_L$ für alle Paare von L und M mit $L \subset M$. Diese Homomorphismen erfüllen offensichtlich die Relationen

$$\phi_{L,L} = \mathrm{id}_{G_L} \quad \text{und} \quad \phi_{L,N} = \phi_{L,M} \circ \phi_{M,N}$$

wenn $L \subset M \subset N$. Außerdem gibt es zu je zwei endlichen Galoiserweiterungen L_1 und L_2 immer eine endliche Galoiserweiterung M (z.B. das Kompositum L_1L_2) mit $L_1, L_2 \subset M$. All das zusammen bildet ein Beispiel für ein projektives (oder inverses) System:

Definition 4.12.

(1) Eine (partiell) geordnete Menge I heißt *nach oben filtriert*, wenn es zu $i_1, i_2 \in I$ stets ein $j \in I$ gibt mit $i_1, i_2 \leq j$ (d.h. je zwei Elemente haben eine gemeinsame obere Schranke in I).

(2) Ein *projektives System* von Gruppen besteht aus einer nach oben filtrierten geordneten Menge I, einer Familie $(G_i)_{i\in I}$ von Gruppen und einer Familie $(\phi_{ij})_{i\leq j}$ von Gruppenhomomorphismen $\phi_{ij} : G_j \to G_i$, die miteinander kompatibel sind:

$$\phi_{ii} = \mathrm{id}_{G_i}\,, \quad \phi_{ik} = \phi_{ij} \circ \phi_{jk} \text{ für } i \leq j \leq k.$$

(3) Der *projektive Limes* eines projektiven Systems wie in (2) ist eine Gruppe G zusammen mit einer Familie $(\phi_i)_{i\in I}$ von Gruppenhomomorphismen $\phi_i : G \to G_i$, so daß gilt

$$\phi_i = \phi_{ij} \circ \phi_j \quad \text{für alle } i \leq j\,,$$

und so daß für jedes andere Paar $(G', (\phi'_i))$ mit diesen Eigenschaften ein eindeutig bestimmter Gruppenhomomorphismus $\varphi : G' \to G$ existiert mit $\phi'_i = \phi_i \circ \varphi$ für alle $i \in I$. Man schreibt kurz $G = \varprojlim G_i$ (die Homomorphismen sind üblicherweise klar aus dem Kontext).

Es folgt, daß der projektive Limes (wenn er existiert) bis auf (eindeutigen) Isomorphismus eindeutig bestimmt ist.

(4) Die Definitionen von *injektivem System* und *injektivem Limes* erhält man, wenn man in obigen Definitionen die Pfeile umdreht. Die Schreibweise ist dementsprechend $G = \varinjlim G_i$.

Die Frage ist jetzt natürlich, ob solche Limiten immer existieren. Die Antwort ist Ja.

PROPOSITION 4.13.

(1) *Jedes projektive System* $((G_i),(\phi_{ij}))$ *von Gruppen hat einen projektiven Limes. Er kann wie folgt konstruiert werden:*

$$G = \{(g_i) \in \prod_{i\in I} G_i \mid \phi_{ij}(g_j) = g_i \text{ für alle } i \leq j\}$$

mit $\phi_i = i$*-te Projektion.*

(2) *Jedes injektive System* $((G_i),(\phi_{ij}))$ *von Gruppen hat einen injektiven Limes. Er kann wie folgt konstruiert werden:*

$$G = \coprod_{i\in I} G_i \;/\; \langle \iota_i(g)\iota_j(\phi_{ij}(g))^{-1} \mid i \leq j, g \in G_i\rangle$$

mit ϕ_i *induziert von der kanonischen Einbettung* ι_i *von* G_i *in die direkte Summe* $\coprod_{i\in I} G_i$*.*

BEWEIS: Übung. □

Bekannte Beispiele für projektive Limites sind die p-adischen Zahlen $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ und die Potenzreihen $k[\![T]\!] = \varprojlim k[T]/(T^n)$, beides projektive Limites von Ringen. Für unsere Zwecke ist folgender Spezialfall wichtig.

DEFINITION 4.14. Eine Gruppe, die projektiver Limes von endlichen Gruppen ist, heißt *pro-endliche Gruppe* (engl. pro-finite group).

Zum Beispiel ist $\mathbb{Z}_p$ als additive Gruppe eine pro-endliche Gruppe (sogar eine pro-p-Gruppe als Limes von endlichen p-Gruppen).

PROPOSITION 4.15.

(1) *Eine pro-endliche Gruppe ist der projektive Limes ihrer endlichen Quotienten.*

(2) *Eine pro-endliche Gruppe* G *ist in natürlicher Weise eine kompakte, total unzusammenhängende topologische Gruppe.*

BEWEIS: (1) Übung.
(2) Nach (1) ist $G = \varprojlim G/H$, wo H alle Normalteiler von G von endlichem Index durchläuft. Nach Prop. 4.13 ist G dann in natürlicher Weise eingebettet in das Produkt $\prod_H G/H$. Wenn wir dieses Produkt mit der Produkttopologie bezüglich der diskreten Topologie auf den Faktoren G/H versehen, wird G eine abgeschlossene Untergruppe einer kompakten topologischen Gruppe, ist also selbst kompakt. Da das Produkt total unzusammenhängend ist, gilt dies auch für G. □

BEMERKUNGEN 4.16.

(1) In einer pro-endlichen Gruppe sind die offenen Untergruppen genau die Untergruppen von endlichem Index. (Eine solche enthält einen Normalteiler von endlichem Index, ist also offen als Vereinigung von endlich vielen seiner Nebenklassen. Umgekehrt induziert eine offene Untergruppe eine offene Überdeckung der Gruppe durch ihre Nebenklassen; wegen der Kompaktheit muß die Untergruppe dann endlichen Index haben.)

(2) Ist G eine beliebige Gruppe, so kann man ebenfalls $\hat{G} = \varprojlim G/H$ betrachten (wo H wieder alle Normalteiler von G von endlichem Index durchläuft). $\hat{G}$ heißt dann die *pro-endliche Komplettierung* von G. Beispielsweise ist

$$\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z} = \prod_p \mathbb{Z}_p$$

(nach dem Chinesischen Restsatz).

(3) Zu Teil (2) obiger Proposition gilt auch die Umkehrung: Eine topologische Gruppe, die kompakt und total unzusammenhängend ist, ist pro-endlich.

3.2. Unendliche Galoistheorie. Wir wollen diese Theorie jetzt anwenden auf unendliche Galoiserweiterungen. Sei also L/K eine Galoiserweiterung, d.h. L/K ist algebraisch, separabel und normal, aber nicht notwendig endlich.

PROPOSITION 4.17.

(1) *Für die Galoisgruppe gilt* $\mathrm{Gal}(L/K) = \varprojlim \mathrm{Gal}(M/K)$*, wo* $K \subset M \subset L$ *durch alle endlichen Galoisschen Zwischenkörper läuft. Insbesondere ist* $\mathrm{Gal}(L/K)$ *eine pro-endliche Gruppe.*

(2) *Die übliche Galoiskorrespondenz liefert eine ordnungsumkehrende Bijektion zwischen den Zwischenkörpern* $K \subset M \subset L$ *und den* abgeschlossenen *Untergruppen von* $\mathrm{Gal}(L/K)$*.*

BEWEIS: (1) Wir haben (durch Einschränkung) Abbildungen $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$, so daß wir jedenfalls einen Homomorphismus $\mathrm{Gal}(L/K) \to \varprojlim \mathrm{Gal}(M/K)$ bekommen. (Allgemein hat man immer einen Homomorphismus $G \to \hat{G}$.) Dieser Homomorphismus ist injektiv: Ist $\mathrm{id}_L \neq \sigma \in \mathrm{Gal}(L/K)$, dann gibt es $\alpha \in L$ mit $\sigma(\alpha) \neq \alpha$. Außerdem liegt α schon in einer endlichen Galoiserweiterung M; dann ist das Bild von σ in $\mathrm{Gal}(M/K)$ nichttrivial. Der Homomorphismus ist surjektiv, weil $L = \bigcup M$ ist — jedes kompatible System von Automorphismen der Zwischenkörper M definiert einen Automorphismus von L.
(2) Siehe [CF, V.1]. □

Zum Beispiel gilt also für die absolute Galoisgruppe eines Körpers K:

$$\mathrm{Gal}_K = \mathrm{Gal}(K^{\mathrm{sep}}/K) = \varprojlim \mathrm{Gal}(L/K)\,,$$

wo $L \subset K^{\mathrm{sep}}$ alle endlichen Galoiserweiterungen von K durchläuft. Dabei ist K^{sep} der separable Abschluß von K, das ist dasselbe wie der algebraische Abschluß, wenn K perfekt ist, also z.B. in Charakteristik 0. Wir werden im Folgenden der Einfachheit halber annehmen, daß K perfekt ist. Wenn man beliebige Körper zulassen will, muß man jeweils $\bar{K}$ durc K^{sep} ersetzen.

Ein konkretes Beispiel für eine absolute Galoisgruppe ist $\mathrm{Gal}_{\mathbb{F}_p} \cong \hat{\mathbb{Z}}$.

3.3. Galoiskohomologie. Im wesentlichen bekommt man die Galoiskohomologie, indem man die Gruppenkohomologie der absoluten Galoisgruppe eines Körpers betrachtet. Da diese absolute Galoisgruppe aber die zusätzliche Struktur einer pro-endlichen Gruppe besitzt, möchte man das berücksichtigen und muß die Definition daher etwas modifizieren. Zunächst macht man eine Einschränkung an die Moduln, die man betrachtet.

DEFINITION 4.18. Sei G eine pro-endliche Gruppe. Ein G-Rechtsmodul M heißt *diskret*, wenn er die folgenden äquivalenten Bedingungen erfüllt.

(1) $M = \bigcup_H M^H$, wobei H durch alle Normalteiler von endlichem Index (d.h. alle offenen Normalteiler) läuft.
(2) Für jedes $m \in M$ ist der Stabilisator $G_m \subset G$ von endlichem Index (d.h. offen).
(3) Die Operation $M \times G \to M$ ist stetig, wobei M die diskrete Topologie trägt.

Der Beweis der Äquivalenz dieser drei Aussagen sei als Übung enpfohlen.

Es gibt nun zwei Möglichkeiten, die Kohomologie einer pro-endlichen Gruppe mit Werten in einem diskreten Modul zu definieren:

1. Möglichkeit: Man betrachtet in der Definition von H^1 nur *stetige* Kozykel (Koränder sind immer stetig); der Modul trägt dabei wie immer die diskrete Topologie. Mit dieser Modifikation geht die gesamte Konstruktion genauso durch wie im schon behandelten Fall der abstrakten Gruppen, denn alles, was wir getan haben, erhält die Stetigkeit. Insbesondere haben wir auch in dieser Theorie die lange exakte Kohomologiesequenz und die Inflations-Restriktions-Sequenz.

2. Möglichkeit: Man betrachtet die endlichen Teilstücke $H^1(G/H, M^H)$ für Normalteiler $H \subset G$ von endlichem Index. Für $H_1 \subset H_2$ hat man dann die Inflationsabbildung $H^1(G/H_2, M^{H_2}) \to H^1(G/H_1, M^{H_1})$; insgesamt erhält man ein injektives System von Kohomologiegruppen, indiziert durch die endlichen Quotienten G/H (oder durch die Normalteiler von endlichem Index mit umgekehrter Ordnung: $H_1 \leq H_2$, wenn $H_1 \supset H_2$). Man kann dann definieren

$$H^1(G, M) = \varinjlim H^1(G/H, M^H)\,.$$

Die wichtige Beobachtung ist dann, daß für diskrete Moduln beide Definitionen übereinstimmen. Wir wollen das hier nicht beweisen, sondern nur bemerken, daß ein stetiger Kozykel stets über einen endlichen Quotienten G/H faktorisiert, was die Identifikation wenigstens plausibel macht.

Der Spezialfall, der uns interessiert, ist, daß die pro-endliche Gruppe G die absolute Galoisgruppe eines Körpers K ist. Es hat sich eingebürgert, in diesem Fall kurz

$$H^1(K, M) \quad \text{für} \quad H^1(\mathrm{Gal}_K, M)$$

zu schreiben. Außerdem schreibt man (in Anlehnung an die Notation für rationale Punkte auf Kurven) meistens

$$M(L) \quad \text{für} \quad M^{\mathrm{Gal}(\bar{K}/L)}\,.$$

Die Inflations-Restriktions-Sequenz lautet dann in ihrem wichtigsten Anwendungsfall

$$0 \longrightarrow H^1(\mathrm{Gal}(L/K), M(L)) \longrightarrow H^1(K, M) \longrightarrow H^1(L, M)\,.$$

3.4. Beispiele. Beispiele von diskreten Galoismoduln sind:

(1) Jeder endliche Galoismodul M, zum Beispiel $M = \mu_n$ (die Gruppe der n-ten Einheitswurzeln, wenn $\mathrm{char}(K) \nmid n$), oder $M = E[n]$ (die n-Torsion einer elliptischen Kurve über K).
(2) Die additive Gruppe $\bar{K}$.
(3) Die multiplikative Gruppe $\bar{K}^\times$.
(4) Die Gruppe $E(\bar{K})$ der algebraischen Punkte auf einer elliptischen Kurve E/K.

Die wichtigsten Grundaussagen über die Kohomologie der additiven und der multiplikativen Gruppe sind wie folgt.

PROPOSITION 4.19.

(1) $H^1(K, \bar{K}) = 0$.
(2) $H^1(K, \bar{K}^\times) = 0$ *(„Satz 90 von Hilbert“).*

BEWEIS: (1) Da $H^1(K, \bar{K}) = \varinjlim H^1(\mathrm{Gal}(L/K), L)$, genügt es zu zeigen, daß $H^1(\mathrm{Gal}(L/K), L) = 0$ ist für jede Galoiserweiterung L/K. Sei $G = \mathrm{Gal}(L/K)$. Nach dem Normalbasissatz gibt es $\alpha \in L$, so daß $(\alpha^\sigma)_{\sigma\in G}$ eine K-Basis von L ist. Anders gesagt, $L \cong K[G] = K \otimes_{\mathbb{Z}} \mathbb{Z}[G]$. Es ist ein allgemeines Resultat, daß für $\mathbb{Z}$-Moduln M gilt $H^1(G, M \otimes_{\mathbb{Z}} \mathbb{Z}[G]) = 0$; siehe Lemma unten.
(2) Es genügt wieder zu zeigen, daß $H^1(G, L^\times) = 0$ ist mit L und G wie oben. Sei dazu $\xi \in Z^1(G, L^\times)$ ein Kozykel. Wegen der linearen Unabhängigkeit der Automorphismen (ein Standardresultat der Galoistheorie) gibt es ein $\beta \in L$, so daß

$$\alpha = \sum_{\sigma\in G} \xi_\sigma \, \beta^\sigma \neq 0$$

ist. Für $\tau \in G$ gilt dann

$$\alpha^\tau = \sum_{\sigma} \xi_\sigma^\tau \, \beta^{\sigma\tau} = \sum_{\sigma} \xi_{\sigma\tau}\xi_\tau^{-1}\beta^{\sigma\tau} = \xi_\tau^{-1}\alpha \,,$$

also ist $\xi_\tau = (\alpha^{-1})^\tau/\alpha^{-1}$ ein Korand. □

LEMMA 4.20. *Sei G eine Gruppe, M ein $\mathbb{Z}$-Modul. Dann ist $M \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ ein G-Rechtsmodul, und es gilt*

$$H^0(G, M \otimes_{\mathbb{Z}} \mathbb{Z}[G]) \cong M \quad \textit{und} \quad H^1(G, M \otimes_{\mathbb{Z}} \mathbb{Z}[G]) = 0 \,.$$

BEWEIS: Sei $M' = M \otimes_{\mathbb{Z}} \mathbb{Z}[G]$. Als abelsche Gruppe ist M' eine direkte Summe von Kopien von M, indiziert durch die Elemente von G. Die G-Operation ist dann gegeben durch

$$(m_\sigma)_{\sigma\in G}^\tau = (m_{\sigma\tau^{-1}})_{\sigma\in G} \,.$$

Damit ist schon klar, daß die Invarianten $(M')^G$ gerade die diagonal eingebetteten Elemente von m sind: $(M')^G = \{(m)_{\sigma\in G} \mid m \in M\} \cong M$. Sei nun $\xi \in Z^1(G, M')$ ein Kozykel. Wir schreiben $\xi_\sigma = (m_{\sigma,\rho})_{\rho\in G}$; dann folgt aus der Kozykelrelation, daß

$$m_{\sigma\tau,\rho} = m_{\sigma,\rho\tau^{-1}} + m_{\tau,\rho} \,, \quad \text{also insbesondere} \quad m_{\sigma,\rho} = m_{\sigma\rho^{-1},1} - m_{\rho^{-1},1} \,.$$

Der Kozykel ist also durch seine Komponenten $m_{\sigma,1}$ bestimmt. Wir betrachten nun

$$\mu = (m_{\rho^{-1},1})_{\rho\in G} \in M' .$$

Es ergibt sich

$$\mu^\sigma - \mu = (m_{(\rho\sigma^{-1})^{-1},1} - m_{\rho^{-1},1})_{\rho\in G} = (m_{\sigma_\rho})_{\rho\in G} = \xi_\sigma ,$$

also ist ξ ein Korand. □

Der ursprüngliche „Satz 90“ aus Hilberts Zahlbericht ist der Spezialfall einer zyklischen Galoiserweiterung: Ist L/K zyklisch vom Grad n, und ist σ ein Erzeuger der Galoisgruppe $\mathrm{Gal}(L/K)$, dann hat jedes $\alpha \in L$ mit $\mathrm{N}_{L/K}(\alpha) = 1$ die Form $\alpha = \beta^\sigma/\beta$ für ein $\beta \in L$.

Damit kann man nun zum Beispiel die Gruppe $H^1(K, \mu_n)$ bestimmen.

Korollar 4.21. *Sei n eine natürliche Zahl, die nicht von $\mathrm{char}(K)$ geteilt wird. Dann ist die Abbildung*

$$K^\times/(K^\times)^n \longrightarrow H^1(K, \mu_n) ,$$

die die Klasse von $\alpha \in K^\times$ abbildet auf die Klasse des Kozykels $\xi_\sigma = \beta^\sigma/\beta$ mit $\beta \in \bar K$, $\beta^n = \alpha$, ein Isomorphismus.

Beweis: Wir betrachten die kurze exakte Sequenz diskreter Galoismoduln

$$0 \longrightarrow \mu_n \longrightarrow \bar K^\times \xrightarrow{x\mapsto x^n} \bar K^\times \longrightarrow 0 .$$

Ein Ausschnitt der langen exakten Kohomologiesequenz dazu lautet

$$K^\times \xrightarrow{x\mapsto x^n} K^\times \xrightarrow{\delta} H^1(K, \mu_n) \longrightarrow H^1(K, \bar K^\times) = 0 .$$

Die Behauptung folgt, wenn man die Definition des verbindenden Homomorphismus δ berücksichtigt. □

Wenn $\mu_n \subset K$ ist, dann ist $H^1(K, \mu_n) = \mathrm{Hom}(\mathrm{Gal}_K, \mathbb{Z}/n\mathbb{Z})$ (denn dann ist μ_n ein trivialer Galoismodul), und man bekommt eine Dualität zwischen der Galoisgruppe der maximalen abelschen Erweiterung von K vom Exponenten n und $K^\times/(K^\times)^n$. Endliche abelsche Erweiterungen von K vom Exponenten n werden also durch endliche Untergruppen von $K^\times/(K^\times)^n$ klassifiziert. Das ist die sogenannte *Kummer-Theorie*. Genauer besagt sie folgendes.

Satz 4.22. *Sei K ein Körper mit $\mu_n \subset K$. Dann gibt es eine Bijektion*

$$\begin{array}{rcl} \{L/K \text{ abelsch, vom Exponenten } n\} & \longleftrightarrow & \{U \subset K^\times/(K^\times)^n \text{ Untergruppe}\} \\ L & \longmapsto & U_L = (K^\times \cap (L^\times)^n)/(K^\times)^n \\ L_U = K(\sqrt[n]{U}) & \longmapsfrom & U \end{array}$$

Außerdem gilt $\mathrm{Gal}(L/K) \cong \mathrm{Hom}(U_L, \mu_n)$.

Beweis: Sei

$$H = \bigcap_{\phi\in\mathrm{Hom}(\mathrm{Gal}_K,\mu_n)} \ker\phi ;$$

dann ist H ein abgeschlossener Normalteiler von Gal_K, gehört also nach Prop. 4.17 zu einer Galoiserweiterung $L_{\max}/K$, d.h. $H = \mathrm{Gal}_{L_{\max}}$. Dann induziert der Isomorphismus $\mathrm{Hom}(\mathrm{Gal}_K, \mu_n) \cong K^\times/(K^\times)^n$ eine perfekte Paarung

$$\kappa : \mathrm{Gal}(L_{\max}/K) \times K^\times/(K^\times)^n \longrightarrow \mu_n , \qquad (\sigma, \alpha(K^\times)^n) \longmapsto \sqrt[n]{\alpha}^\sigma/\sqrt[n]{\alpha} .$$

Denn nach Definition ist $\mathrm{Gal}(L_{\max}/K)$ der maximale abelsche Quotient vom Exponenten n von Gal_K. *Perfekte Paarung* bedeutet, daß κ bilinear ist (beide Gruppen links sind abelsch, also $\mathbb{Z}$-Moduln) und daß gilt

$$\kappa(\sigma,u)=1 \text{ für alle } \sigma\in\mathrm{Gal}(L_{\max}/K) \Longrightarrow u=1\,;$$
$$\kappa(\sigma,u)=1 \text{ für alle } u\in K^\times/(K^\times)^n \Longrightarrow \sigma=1\,.$$

Das folgt aus $\mathrm{Hom}(\mathrm{Gal}_K,\mu_n)\cong K^\times/(K^\times)^n$ und der Definition von $L_{\max}$.

Nach Definition von κ gilt $\kappa(\sigma,u)=1$ genau dann, wenn $\sqrt[n]{u}$ von σ fixiert wird. Also folgt

$$\begin{aligned} U_L &= (K^\times\cap(L^\times)^n)/(K^\times)^n \\ &= \{u\in K^\times/(K^\times)^n \mid \sqrt[n]{u}\in L\} \\ &= \{u\in K^\times/(K^\times)^n \mid \kappa(\sigma,u)=1 \text{ für alle } \sigma\in\mathrm{Gal}(L_{\max}/L)\}\,. \end{aligned}$$

Da κ perfekt ist, bekommen wir jedenfalls schon einmal die Isomorphie

$$\mathrm{Gal}(L/K)=\mathrm{Gal}(L_{\max}/K)/\mathrm{Gal}(L_{\max}/L)\cong\mathrm{Hom}(U_L,\mu_n)\,.$$

(Insbesondere gilt für L/K endlich, daß $[L:K]=\#U_L$.)

Sei umgekehrt $U\subset K^\times/(K^\times)^n$. Dann gilt für $\sigma\in\mathrm{Gal}(L_{\max}/K)$, daß σ L_U fixiert genau dann, wenn σ alle $\sqrt[n]{u}$ für $u\in U$ fixiert, und das gilt genau dann, wenn $\kappa(\sigma,u)=1$ ist für alle $u\in U$. Aus der Perfektheit von κ folgt dann wie eben die Isomorphie $\mathrm{Gal}(L_U/K)\cong\mathrm{Hom}(U,\mu_n)$.

Da $L_{U_L}\subset L$, haben wir einen Epimorphismus $\mathrm{Gal}(L/K)\twoheadrightarrow\mathrm{Gal}(L_{U_L}/K)$; andererseits sind die beiden Galoisgruppen aber nach dem oben Gesagten isomorph. Also gilt $L_{U_L}=L$. Genauso zeigt man $U_{L_U}=U$. □

Die Bedeutung dieses Ergebnisses liegt darin, daß es sämtliche abelschen Erweiterungen von Exponenten n in einer sehr expliziten und konstruktiven Weise klassifiziert. Wir werden davon gleich noch Gebrauch machen.

Wir können die Überlegung, die zur Bestimmung von $H^1(K,\mu_n)$ geführt hat, auch auf elliptische Kurven anwenden.

PROPOSITION 4.23. *Sei E/K eine elliptische Kurve und n eine natürliche Zahl, die nicht von* $\mathrm{char}(K)$ *geteilt wird. Dann haben wir eine kurze exakte Sequenz*

$$0\longrightarrow E(K)/nE(K)\longrightarrow H^1(K,E[n])\longrightarrow H^1(K,E(\bar K))[n]\longrightarrow 0\,.$$

BEWEIS: Wie oben betrachten wir die kurze exakte Sequenz diskreter Galoismoduln

$$0\longrightarrow E[n]\longrightarrow E(\bar K)\overset{P\mapsto nP}{\longrightarrow} E(\bar K)\longrightarrow 0\,.$$

Die lange exakte Kohonologiesequenz liefert dann die Behauptung. □

Ein Weg, die Endlichkeit von $E(K)/nE(K)$ zu zeigen, ist also, das Bild dieser Gruppe in $H^1(K,E[n])$ geeignet zu beschränken. Anders als im Fall der multiplikativen Gruppe verschwindet $H^1(K,E(\bar K))$ nicht, sondern ist sehr groß (isomorph zur Weil-Chatelet-Gruppe der Isomorphieklassen von prinzipal homogenen Räumen für E), so daß für Zahlkörper K die Gruppe $H^1(K,E[n])$ unendlich ist. Man muß also noch etwas mehr arbeiten, um die Endlichkeit von $E(K)/nE(K)$ nachzuweisen.

4. Unverzweigte Erweiterungen

4.1. Verzweigung von Primidealen (Kurzfassung). Sei L/K eine endliche Erweiterung von algebraischen Zahlkörpern, und sei $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal. Dann ist $\mathfrak{p}\mathcal{O}_L$ ein Ideal in $\mathcal{O}_L$, und nach dem Satz von der eindeutigen Primidealzerlegung in Dedekindringen (siehe z.B. [Neu, I.3.9]) haben wir eine Produktdarstellung

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_g^{e_g}$$

mit paarweise verschiedenen Primidealen $\mathfrak{P}_j \subset \mathcal{O}_L$ und ganzen Zahlen $e_j \geq 1$. Von den Primidealen $\mathfrak{P}_j$ sagt man, sie lägen *über* $\mathfrak{p}$ und schreibt $\mathfrak{P}_j \mid \mathfrak{p}$. Wir schreiben auch $e_{\mathfrak{P}/\mathfrak{p}} = e_j$ für $\mathfrak{P} = \mathfrak{P}_j$.

Für $\alpha \in K^\times$ ist die $\mathfrak{p}$-*adische Bewertung* definiert als

$$v_\mathfrak{p}(\alpha) = \max\{n \in \mathbb{Z} \mid \alpha \in \mathfrak{p}^n\};$$

das ist dasselbe wie der Exponent von $\mathfrak{p}$ in der Primidealzerlegung des Hauptideals $\alpha\mathcal{O}_K$.

Literatur zur Verzweigungstheorie sind zum Beispiel die Abschnitte 8 und 9 im Kapitel I von [Neu].

Definition 4.24.

(1) $\mathfrak{P}_j$ heißt *verzweigt (ramified)* über $\mathfrak{p}$, wenn $e_j > 1$.
(2) $\mathfrak{p}$ heißt in L/K *verzweigt*, und L/K heißt *verzweigt* bei $\mathfrak{p}$, wenn $e_j > 1$ für ein j.
(3) *Unverzweigt* heißt nicht verzweigt.
(4) Sei S eine Menge von Primidealen von $\mathcal{O}_K$. Dann heißt L/K *unverzweigt außerhalb von* S, wenn alle in L/K verzweigten Primidale $\mathfrak{p} \subset \mathcal{O}_K$ in S liegen.

Aus vorhandenen unverzweigten Erweiterungen lassen sich neue gewinnen:

Lemma 4.25.

(1) *Ist L/K unverzweigt bei $\mathfrak{p}$ und $K \subset K' \subset L$, so ist K'/K ebenfalls unverzweigt bei $\mathfrak{p}$.*
(2) *Sind K_1/K unverzweigt bei $\mathfrak{p}$ und K_2/K_1 unverzweigt bei allen $\mathfrak{P} \mid \mathfrak{p}$, so ist K_2/K unverzweigt bei $\mathfrak{p}$.*
(3) *Ist K'/K unverzweigt bei $\mathfrak{p}$, und ist L/K eine endliche Erweiterung, dann ist LK'/L unverzweigt bei allen $\mathfrak{P} \mid \mathfrak{p}$.*
(4) *Sind K_1/K und K_2/K unverzweigt bei $\mathfrak{p}$, so ist auch K_1K_2/K unverzweigt bei $\mathfrak{p}$.*

Die letzte Eigenschaft ermöglicht es, auch für unendliche Erweiterungen zu definieren, was „unverzweigt“ bedeutet.

Definition 4.26. Eine eventuell unendliche algebraische Erweiterung L/K eines Zahlkörpers K heißt *unverzweigt* bei $\mathfrak{p}$, wenn alle ihre endlichen Teilerweiterungen bei $\mathfrak{p}$ unverzweigt sind.

Zu einer Menge S von Primidealen von $\mathcal{O}_K$ gibt es dann eine maximale außerhalb von S unverzweigte Erweiterung.

Wenn L/K Galoissch ist, kann man zeigen, daß die Galoisgruppe auf den Primidealen über $\mathfrak{p}$ transitiv operiert. Insbesondere sind dann alle $e_j = e$ gleich. Das Verzweigungsverhalten läßt sich dann auch durch Untergruppen der Galoisgruppe ausdrücken.

DEFINITION 4.27. Seien L/K Galoissch und $\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{P} \subset \mathcal{O}_L$ Primideale mit $\mathfrak{P} \mid \mathfrak{p}$.

(1) $D_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \mathfrak{P}^\sigma = \mathfrak{P}\}$ heißt die *Zerlegungsgruppe (decomposition group)* von $\mathfrak{P}$. Jedes $\sigma \in D_{\mathfrak{P}}$ induziert einen Automorphismus der Restklassenkörpererweiterung $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$; wir erhalten also einen (surjektiven) Homomorphismus

$$D_{\mathfrak{P}} \longrightarrow \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))\,.$$

(2) Die *Trägheitsgruppe (inertia group)* von $\mathfrak{P}$, $I_{\mathfrak{P}}$, ist der Kern des obigen Homomorphismus. Sei kann auch definiert werden als

$$I_{\mathfrak{P}} = \{\sigma \in D_{\mathfrak{P}} \mid x^\sigma \equiv x \bmod \mathfrak{P} \text{ für alle } x \in \mathcal{O}_L\}\,.$$

Den Zusammenhang mit dem Verzweigungsverhalten liefert folgendes Lemma.

LEMMA 4.28. *Sei L/K Galoissch und $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal. Dann ist $\mathfrak{p}$ in L/K genau dann unverzweigt, wenn für ein (oder alle) $\mathfrak{P} \mid \mathfrak{p}$ die Trägheitsgruppe $I_{\mathfrak{P}}$ trivial ist.*

Das nächste Lemma stellt einen Zusammenhang her mit den Bewertungen.

LEMMA 4.29. *$\mathfrak{P} \mid \mathfrak{p}$ ist in L/K genau dann unverzweigt, wenn für alle $\alpha \in K$ gilt, daß $v_{\mathfrak{P}}(\alpha) = v_{\mathfrak{p}}(\alpha)$.*

BEWEIS: Beachte

$$\alpha\mathcal{O}_L = (\alpha\mathcal{O}_K)\mathcal{O}_L = (\ldots\mathfrak{p}^{v_{\mathfrak{p}}(\alpha)}\ldots)\mathcal{O}_L = \ldots\mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}v_{\mathfrak{p}}(\alpha)}\ldots\,,$$

also ist $v_{\mathfrak{P}}(\alpha) = e_{\mathfrak{P}/\mathfrak{p}}v_{\mathfrak{p}}(\alpha)$, woraus die Behauptung folgt. □

Schließlich brauchen wir noch ein Kriterium, anhand dessen wir bei einer konkret gegebenen Erweiterung feststellen können, daß ein Primideal unverzweigt ist.

LEMMA 4.30. *Sei $L = K(\alpha)$, wo α Nullstelle des normierten Polynoms $f \in \mathcal{O}_K[X]$ ist. Sei $\mathfrak{p}$ ein Primideal von $\mathcal{O}_K$, so daß die Reduktion von f, $\bar{f} \in \mathcal{O}_K/\mathfrak{p}[X]$, keine mehrfachen Nullstellen (im algebraischen Abschluß von $\mathcal{O}_K/\mathfrak{p}$) hat. Dann ist L/K bei $\mathfrak{p}$ unverzweigt.*

BEWEIS: Wir zeigen, daß der Zerfällungskörper M von f (der L enthält) bei $\mathfrak{p}$ unverzweigt ist. Dazu bemerken wir, daß Reduktion modulo $\mathfrak{P}$ (für ein Primideal $\mathfrak{P} \mid \mathfrak{p}$ von $\mathcal{O}_M$) eine Bijektion zwischen den Nullstellen von f in M und den Nullstellen von $\bar{f}$ in $\mathcal{O}_M/\mathfrak{P}$ induziert, die außerdem mit der Operation von $D_{\mathfrak{P}}$ verträglich ist. Es folgt, daß jedes Element von $I_{\mathfrak{P}}$ auf den Nullstellen von f trivial operiert, also auch auf M, d.h., $I_{\mathfrak{P}}$ ist trivial. Nach Lemma 4.28 folgt die Behauptung. □

4.2. Ein Endlichkeitsresultat. Für uns ist jetzt folgendes fundamentale Endlichkeitsresultat wichtig.

SATZ 4.31. *Sei K ein algebraischer Zahlkörper, S eine endliche Menge von Primidealen von $\mathcal{O}_K$ und $n \geq 2$ eine natürliche Zahl. Sei L/K die maximale abelsche Erweiterung vom Exponenten n, die außerhalb von S unverzweigt ist. Dann ist L/K endlich.*

BEWEIS: 1. Schritt: Wir zeigen, daß wir ohne Einschränkung $\mu_n \subset K$ annehmen können. Sei dazu $K' = K(\mu_n)$ und S' die Menge der Primideale $\mathfrak{P}$ von $\mathcal{O}_{K'}$ mit $\mathfrak{P} \mid \mathfrak{p}$ für ein $\mathfrak{p} \in S$. Sei L'/K' die maximale abelsche Erweiterung vom Exponenten n, die außerhalb von S' unverzweigt ist. Wir setzen voraus, daß L'/K' endlich ist. Dann ist L'/K ebenfalls endlich, und da LK'/K' eine abelsche Erweiterung vom Exponenten n, unverzweigt außerhalb von S', ist, folgt $LK' \subset L'$. Damit ist LK'/K endlich, also erst recht L/K endlich.

2. Schritt: Wir nehmen nun an, daß $\mu_n \subset K$ ist. Indem wir S eventuell vergrößern (was L nur größer machen kann), können wir annehmen, daß $\mathfrak{p} \nmid n$ für alle $\mathfrak{p} \notin S$. Nach Satz 4.22 ist $L = K(\sqrt[n]{U})$ mit einer Untergruppe U von $K^\times/(K^\times)^n$. Nach dem Lemma unten gilt für $\mathfrak{p} \in S$ und $u \in K^\times$, daß $K(\sqrt[n]{u})/K$ genau dann bei $\mathfrak{p}$ unverzweigt ist, wenn $v_\mathfrak{p}(u) \equiv 0 \bmod n$ ist. Also haben wir

$$U = \{u \in K^\times/(K^\times)^n \mid v_\mathfrak{p}(u) \equiv 0 \bmod n \text{ für alle } \mathfrak{p} \notin S\}\,.$$

Mit U ist auch L/K endlich, also genügt es zu zeigen, daß U endlich ist.

3. Schritt: U ist endlich. Dazu sei

$$U_0 = \{u \in K^\times/(K^\times)^n \mid v_\mathfrak{p}(u) \equiv 0 \bmod n \text{ für alle } \mathfrak{p}\}\,.$$

Sei $I(K)$ die Gruppe der gebrochenen Ideale von K und $\mathrm{Cl}(K)$ die Idealklassengruppe von K. Dann haben wir die exakte Sequenz

$$0 \longrightarrow \mathcal{O}_K^\times \longrightarrow K^\times \longrightarrow I(K) \longrightarrow \mathrm{Cl}(K) \longrightarrow 0\,.$$

Das liefert das folgende exakte Diagramm:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathcal{O}_K^\times & \xrightarrow{n} & \mathcal{O}_K^\times & \longrightarrow & U_0 & \dashrightarrow & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & K^\times & \xrightarrow{n} & K^\times & \longrightarrow & K^\times/(K^\times)^n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I(K) & \xrightarrow{n} & I(K) & \longrightarrow & I(K)/I(K)^n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & \dashrightarrow & \mathrm{Cl}\,K & \xrightarrow{n} & \mathrm{Cl}(k) & \longrightarrow & \mathrm{Cl}(K)/Cl(K)^n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Nach dem Schlangenlemma bekommen wir die kurze exakte Sequenz

$$0 \longrightarrow \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \longrightarrow U_0 \longrightarrow \mathrm{Cl}(K)[n] \longrightarrow 0\,.$$

Nun ist nach dem Dirichletschen Einheitensatz (siehe [**Neu**, I.7]) $\mathcal{O}_K^\times$ endlich erzeugt, also $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n$ endlich. Weiterhin ist ([**Neu**, I.6]) die Idealklassengruppe endlich, also ist auch ihre Untergruppe $\mathrm{Cl}(K)[n]$ endlich. Zusammen folgt, daß U_0 endlich ist. Schließlich haben wir eine exakte Sequenz

$$0 \longrightarrow U_0 \longrightarrow U \longrightarrow \bigoplus_{\mathfrak{p}\in S} \mathbb{Z}/n\mathbb{Z}$$

(die rechte Abbildung ist durch die Bewertungen $v_\mathfrak{p}$ gegeben), was zeigt, daß auch U endlich ist. □

Es fehlt noch das erwähnte Lemma.

LEMMA 4.32. *Sei K ein Zahlkörper, $n \geq 2$ mit $\mu_n \subset K$, sei weiter $\mathfrak{p}$ ein Primideal von $\mathcal{O}_K$ mit $\mathfrak{p} \nmid n$ und $u \in K^\times$. Dann ist $K(\sqrt[n]{u})/K$ genau dann unverzweigt bei $\mathfrak{p}$, wenn $v_\mathfrak{p}(u) \equiv 0 \bmod n$ ist.*

BEWEIS: Sei zunächst $v_\mathfrak{p}(u) = kn$. Es gibt $\pi \in K^\times$ mit $v_\mathfrak{p}(\pi) = 1$. Durch Multiplikation mit $(\pi^{-k})^n$ können wir annehmen, daß $v_\mathfrak{p}(u) = 0$ ist. Weiterhin können wir u mit der n-ten Potenz eines geeigneten Elements $\alpha \in \mathcal{O}_K^\times$ multiplizieren, um zusätzlich $u \in \mathcal{O}_K^\times$ zu erreichen. Dann wird $K(\sqrt[n]{u})$ von einer Nullstelle des Polynoms $f = X^n - u \in \mathcal{O}_K[X]$ erzeugt, und $\bar{f}$ hat keine mehrfachen Nullstellen, da $\bar{f}' = nX^{n-1}$ nur bei 0 verschwindet (hier brauchen wir $\mathfrak{p} \nmid n$). Nach Lemma 4.30 ist dann $K(\sqrt[n]{u})/K$ bei $\mathfrak{p}$ unverzweigt.

Sei nun $K(\sqrt[n]{u})/K$ unverzweigt bei $\mathfrak{p}$ und $\mathfrak{P} \mid \mathfrak{p}$. Dann gilt nach Lemma 4.29

$$v_\mathfrak{p}(u) = v_\mathfrak{P}(u) = nv_\mathfrak{P}(\sqrt[n]{u}) \equiv 0 \bmod n\,.$$

□

4.3. Unverzweigte Kohomologie. Wir können nun definieren, wann eine Kohomologieklasse unverzweigt heißen soll.

DEFINITION 4.33. Sei K ein Zahlkörper und M ein K-Galoismodul.

(1) Sei $\mathfrak{p}$ ein Primideal in $\mathcal{O}_K$. $\xi \in H^1(K, M)$ heißt *in $\mathfrak{p}$ unverzweigt*, wenn es eine bei $\mathfrak{p}$ unverzweigte endliche Galoiserweiterung L/K gibt, so daß ξ im Bild der Inflationsabbildung $H^1(\mathrm{Gal}(L/K), M(L)) \to H^1(K, M)$ liegt, oder äquivalent, wenn ξ durch einen Kozykel repräsentiert wird, der über $\mathrm{Gal}(L/K)$ für eine solche Erweiterung faktorisiert.
(2) Sei S eine Menge von Primidealen von $\mathcal{O}_K$. Dann heißt $\xi \in H^1(K, M)$ *unverzweigt außerhalb von S*, wenn alle Primideale, bei denen ξ nicht unverzweigt ist, in S liegen. Wir schreiben $H^1(K, M; S)$ für die Untergruppe der außerhalb von S unverzweigten Kohomologieklassen.

Aus dem Endlichkeitsresultat über unverzweigte Erweiterungen im vorigen Abschnitt folgt nun ein Endlichkeitsresultat über unverzweigte Kohomologiegruppen.

SATZ 4.34. *Sei K ein Zahlkörper, M ein endlicher K-Galoismodul und S eine endliche Menge von Primidealen von $\mathcal{O}_K$. Dann ist $H^1(K, M; S)$ endlich.*

BEWEIS: Sei L/K eine endliche Galoiserweiterung, so daß M ein trivialer L-Galoismodul ist. (So ein L existiert, da M endlich ist.) Setze

$$S_L = \{\mathfrak{P} \text{ Primideal von } \mathcal{O}_L \mid \mathfrak{P}|\mathfrak{p}\}\,.$$

Dann ist das Bild von $H^1(K, M; S)$ unter $\mathrm{res}_{L/K}$ in $H^1(L, M; S_L)$ enthalten: Sei $\xi \in H^1(K, M; S)$ und $\mathfrak{p} \notin S$ ein Primideal von $\mathcal{O}_K$; dann gibt es K'/K endlich, in $\mathfrak{p}$ unverzweigt, so daß ξ im Bild von $inf_{K'/K}$ liegt. Wir haben dann ein kommutatives Diagramm

$$\begin{array}{ccc} H^1(K, M) & \xrightarrow{\text{res}} & H^1(L, M) \\ \uparrow{\scriptstyle \text{inf}} & & \uparrow{\scriptstyle \text{inf}} \\ H^1(\mathrm{Gal}(K'/K), M(K')) & \xrightarrow{\text{res}} & H^1(\mathrm{Gal}(LK'/L), M(LK')) \end{array}$$

und nach Lemma 4.25, (3), ist LK'/L bei allen $\mathfrak{P} \mid \mathfrak{p}$ unverzweigt. Also ist $\mathrm{res}(\xi) \in H^1(L, M)$ bei allen diesen $\mathfrak{P}$ unverzweigt.

Aus der Inflations-Restriktions-Sequenz (Prop. 4.11) erhaten wir dann das Diagramm mit exakten Zeilen

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Ker} & \xrightarrow{\text{inf}} & H^1(K, M; S) & \xrightarrow{\text{res}} & H^1(L, M; S_L) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & H^1(\mathrm{Gal}(L/K), M(L)) & \xrightarrow{\text{inf}} & H^1(K, M) & \xrightarrow{\text{res}} & H^1(L, M) \end{array}$$

Da $H^1(\mathrm{Gal}(L/K), M(L))$ endlich ist (endliche Gruppe, endlicher Modul), ist auch Ker endlich. Es genügt also, wenn wir zeigen können, daß $H^1(L, M; S_L)$ endlich ist, d.h. die Behauptung unter der zusätzlichen Annahme, daß der Modul M trivial ist.

Sei also jetzt vorausgesetzt, daß M ein trivialer K-Galoismodul ist. Sei weiter $m \geq 2$ eine ganze Zahl, die M annulliert. Sei dann L/K die maximale abelsche Erweiterung von Exponenten m, die außerhalb von S unverzweigt ist. Nach Satz 4.31 ist L/K dann eine endliche Erweiterung. Da M ein trivialer Modul ist, gilt $H^1(K, M) = \mathrm{Hom}(\mathrm{Gal}_K, M)$ (die Homomorphismen sind dabei stetig, d.h., sie faktorisieren über einen endlichen Quotienten $\mathrm{Gal}(K'/L)$). Für $\xi \in H^1(K, M; S) \subset \mathrm{Hom}(\mathrm{Gal}_K, M)$ sei L_ξ/K die minimale Erweiterung, so daß ξ über $\mathrm{Gal}(L_\xi/K)$ faktorisiert. (D.h., Gal_{L_ξ} ist der Kern von ξ, wenn wir ξ als Homomorphismus interpretieren.) Da ξ außerhalb von S unverzweigt ist, muß L_ξ außerhalb von S unverzweigt sein. Als Homomorphismus induziert ξ eine Einbettung

$$\xi : \mathrm{Gal}(L_\xi/K) = \mathrm{Gal}_K \,/\, \ker \xi \hookrightarrow M\,,$$

also ist L_ξ/K abelsch vom Exponenten m. Alles zusammengenommen heißt das, daß $L_\xi \subset L$ ist. Insbesondere faktorisiert ξ über $\mathrm{Gal}(L/K)$. Wir haben also eine Einbettung $H^1(K, M; S) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(L/K), M)$, also ist $H^1(K, M; S)$ endlich. □

5. Anwendung: Der schwache Satz von Mordell-Weil

Das soeben bewiesene Endlichkeitsresultat wird es uns erlauben, den schwachen Satz von Mordell-Weil zu beweisen. Dazu brauchen wir noch ein Resultat, dessen Beweis wir auf später verschieben.

LEMMA 4.35. *Sei E/K eine elliptische Kurve über einem Zahlkörper, gegeben durch eine Weierstraßgleichung mit Koeffizienten in $\mathcal{O}_K$; sei weiter $\mathfrak{p}$ ein Primideal von $\mathcal{O}_K$ mit Restklassencharakteristik p. Sei $P = (\xi, \eta) \in E(K)$ mit $v_\mathfrak{p}(\xi) < 0$. Dann gilt:*

(1) *Für alle $n \in \mathbb{Z}$ ist $n \cdot P = O$ oder $v_\mathfrak{p}(x(n \cdot P)) \leq v_\mathfrak{p}(\xi)$;*
(2) *$p \cdot P = O$ oder $v_\mathfrak{p}(x(p \cdot P)) < v_\mathfrak{p}(\xi)$.*

PROPOSITION 4.36. *Sei E/K eine elliptische Kurve über einem Zahlkörper, gegeben durch eine Weierstraßgleichung mit Koeffizienten in $\mathcal{O}_K$; sei weiter $\mathfrak{p}$ ein Primideal von $\mathcal{O}_K$ mit Restklassencharakteristik p, und sei $n \in \mathbb{Z}$ eine Zahl, die nicht von p geteilt wird. Dann gilt für alle $P = (\xi, \eta) \in E(K) \setminus \{O\}$ mit $v_\mathfrak{p}(\xi) < 0$, daß $n \cdot P \neq O$ ist.*

BEWEIS: Da p und n relativ prim sind, gibt es nach dem Chinesischen Restsatz ein $a \in \mathbb{Z}$ mit $p \mid a$ und $a \equiv 1 \bmod n$. Wir nehmen an, $n \cdot P = O$. Dann ist $a \cdot P = P$, also

$$v_\mathfrak{p}(\xi) = v_\mathfrak{p}(x(a \cdot P)) = v_\mathfrak{p}(x(p \cdot (a/p) \cdot P)) < v_\mathfrak{p}(x((a/p) \cdot P)) \leq v_\mathfrak{p}(\xi)$$

nach Lemma 4.35, ein Widerspruch. □

Das können wir benutzen, um etwas über das Verzweigungsverhalten des Bildes von $E(K)/nE(K)$ unter dem verbindenden Homomorphismus auszusagen.

PROPOSITION 4.37. *Sei E/K eine elliptische Kurve über einem Zahlkörper, gegeben durch eine Weierstraßgleichung mit Koeffizienten in $\mathcal{O}_K$, und sei $\mathfrak{p}$ ein Primideal von $\mathcal{O}_K$ mit $v_\mathfrak{p}(\Delta_E) = 0$. Sei weiter $n \in \mathbb{Z}$ nicht durch die Restklassencharakteristik p von $\mathfrak{p}$ teilbar. Dann besteht das Bild des verbindenden Homomorphismus in der langen exakten Kohomologiesequenz,*

$$\delta : E(K)/nE(K) \longrightarrow H^1(K, E[n]),$$

aus Kohomologieklassen, die bei $\mathfrak{p}$ unverzweigt sind.

BEWEIS: Sei $P \in E(K)$ und $Q \in E(\bar{K})$ mit $n \cdot Q = P$. Der Körper $K(Q) = K(x(Q), y(Q))$ ist dann eine endliche Erweiterung von K; sei L/K der Galoissche Abschluß von $K(Q)/K$.

Behauptung: L/K ist bei $\mathfrak{p}$ unverzweigt.

Zum Beweis sei $\mathfrak{P}$ ein Primideal von $\mathcal{O}_L$ über $\mathfrak{p}$, $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ und $k_\mathfrak{P} = \mathcal{O}_L/\mathfrak{P}$ seien die Restklassenkörper. Da $v_\mathfrak{p}(\Delta_E) = 0$, bekommen wir eine elliptische Kurve $\tilde{E}$ über $k_\mathfrak{p}$, wenn wir die definierende Gleichung modulo $\mathfrak{p}$ reduzieren. Seien $\tilde{P} \in \tilde{E}(K_\mathfrak{p})$ und $\tilde{Q} \in \tilde{E}(k_\mathfrak{P})$ die Bilder von P und Q auf $\tilde{E}$. Wir zeigen, daß L/K bei $\mathfrak{p}$ unverzweigt ist, indem wir zeigen, daß die Trägheitsgruppe $I_\mathfrak{P}$ trivial ist (siehe Lemma 4.28). Sei dazu $\sigma \in I_\mathfrak{P}$. Nach Definition gilt dann $\tilde{Q}^\sigma = \tilde{Q}$, also

ist $\widetilde{Q^\sigma - Q} = \tilde{O}$. Wenn $Q^\sigma \neq Q$ ist, dann folgt daraus $v_{\mathfrak{P}}(x(Q^\sigma - Q)) < 0$. Nun ist aber

$$n(Q^\sigma - Q) = (nQ)^\sigma - (nQ) = P^\sigma - P = 0\,;$$

das ist ein Widerspruch zu Prop. 4.36. Also ist $Q^\sigma = Q$, d.h., σ operiert trivial auf $K(Q)$. Dasselbe Argument zeigt, daß σ trivial operiert auf allen Konjugierten $K(Q^\tau)$, also operiert σ trivial auf dem Kompositum L dieser Körper. Dann ist σ aber die Identität.

Nach Definition von δ sehen wir, daß $\delta(P)$ im Bild der Inflationsabbildung $H^1(\mathrm{Gal}(L/K), E[n]) \to H^1(K, E[n])$ liegt, also ist $\delta(P)$ bei $\mathfrak{p}$ unverzweigt. □

Nun können wir endlich den schwachen Satz von Mordell-Weil beweisen.

Satz 4.38. *Sei E/K eine elliptische Kurve über einem Zahlkörper, und sei $n \geq 2$ eine natürliche Zahl. Dann ist $E(K)/nE(K)$ endlich.*

Beweis: Sei E durch eine Weierstraßgleichung mit Koeffizienten in $\mathcal{O}_K$ gegeben. Sei weiter S die (endliche) Menge der Primideale $\mathfrak{p}$ von $\mathcal{O}_K$, so daß $v_{\mathfrak{p}}(\Delta_E) > 0$ oder $v_{\mathfrak{p}}(n) > 0$ ist. Dann haben wir nach Prop. 4.37 die Einbettung

$$\delta : E(K)/nE(K) \hookrightarrow H^1(K, E[n]; S)\,,$$

und nach Satz 4.34 ist die rechtsstehende Gruppe endlich. □

6. Die formale Gruppe einer elliptischen Kurve

Um den Beweis des schwachen Satzes von Mordell-Weil zu vervollständigen, bleibt noch der Beweis des Lemmas 4.35 nachzutragen. Dazu geben wir einen kurzen Abriß der Theorie der formalen Gruppe einer elliptischen Kurve. Der Einfachheit halber betrachten wir eine kurze Weierstraß-Gleichung; alles funktioniert aber genauso mit einer langen Weierstraß-Gleichung; lediglich die Formeln werden etwas länger.

6.1. Konstruktion der formalen Gruppe. Sei also $E : y^2 = x^3 + A\,x + B$ eine elliptische Kurve. Wir wollen das Verhalten von E in der Nähe des Nullpunktes O „analytisch“ untersuchen. Dabei ist es unpraktisch, daß in den üblichen affinen Koordinaten der Nullpunkt gerade der Punkt im Unendlichen ist. Deshalb wählen wir ein anderes Koordinatensystem, in dem der Punkt O im Ursprung liegt. Da in projektiven Koordinaten $O = (0 : 1 : 0)$ ist, wählt man die affine Karte mit $Y = 1$. Wir setzen $z = x/y$ und $w = 1/y$ und bekommen die Gleichung

$$E : w = z^3 + A\,w^2 z + B\,w^3\,.$$

Diese Gleichung kann man dazu benutzen, w als Potenzreihe in z auszudrücken (d.h., w als „analytische Funktion“ von z zu schreiben).

Lemma 4.39. *Sei R ein Ring und $F(w, z) \in R[w, z]$ ein Polynom, das sich in der Form $F(w, z) = w^2 F_1(w, z) + zF_2(w, z)$ mit Polynomen F_1, F_2 schreiben läßt. Dann hat die Gleichung*

$$w = F(w, z)$$

genau eine Lösung $w \in zR[\![z]\!]$, und jede Folge

$$w_0, \quad w_1 = F(w_0, z), \quad w_2 = F(w_1, z), \quad \dots$$

konvergiert gegen diese Lösung.

Beweis: Für eine Potenzreihe $f \in R[\![z]\!]$ sei $v(f)$ die Bewertung (oder auch Untergrad), d.h. der kleinste Exponent mit nicht-verschwindendem Koeffizienten (man setzt $v(0) = +\infty$). Dann überlegt man sich leicht, daß $zR[\![z]\!]$ mit der Metrik $d(f,g) = 2^{-v(f-g)}$ einen vollständigen metrischen Raum bildet. Außerdem folgt aus der Voraussetzung an F, daß die Abbildung

$$zR[\![z]\!] \ni w \longmapsto F(w,z) \in zR[\![z]\!]$$

kontrahierend ist. Nach dem Banachschen Fixpunktsatz folgt die Behauptung. □

Wir wenden das auf unsere Gleichung für E an und bekommen eine Entwicklung

(6.1)
$$w(z) = z^3 + A\,z^7 + B\,z^9 + 2\,A^2\,z^{11} + 5\,A\,B\,z^{13} + (5\,A^3 + 3\,B^2)\,z^{15} + O(z^{17})$$

Daraus ergeben sich Laurent-Reihen in z für die üblichen affinen Koordinaten x und y:

(6.2)
$$x(z) = z/w(z) = z^{-2} - A\,z^2 - B\,z^4 - A^2\,z^6 - 3\,A\,B\,z^8 - (2\,A^3 + 2\,B^2)\,z^{10} + O(z^{12})$$

(6.3)
$$y(z) = 1/w(z) = z^{-3} - A\,z - B\,z^3 - A^2\,z^5 - 3\,A\,B\,z^7 - (2\,A^3 + 2\,B^2)\,z^9 + O(z^{11})$$

Man erhält auf diese Weise einen „generischen“ Punkt $P = (x(z), y(z)) \in E(K(\!(z)\!))$. Wie drückt sich nun die Addition auf E in der z-Koordinate aus? Zunächst gilt einfach

$$-P = (x(z), -y(z)), \quad \text{also} \quad z(-P) = -z\,.$$

Seien nun P_1 und P_2 zwei Punkte mit z-Koordinaten z_1 und z_2 (wir können uns $P_j = (x(z_j), y(z_j)) \in E(K(\!(z_1, z_2)\!))$ vorstellen). Wir berechnen $z(P_1 + P_2)$ nach dem üblichen Verfahren. Zunächst bestimmen wir die Gleichung der Geraden $w = \lambda\,z + \mu$ durch die beiden Punkte P_1 und P_2. Die Steigung λ ergibt sich als Differenzenquotient

$$\lambda = \frac{w(z_2) - w(z_1)}{z_2 - z_1} = (z_1^2 + z_1 z_2 + z_2^2) + A\,(z_1^6 + z_1^5 z_2 + \dots + z_1 z_2^5 + z_2^6) + \dots$$

und μ dann aus

$$\mu = w(z_1) - \lambda\,z_1 = -z_1 z_2 (z_1 + z_2) - A\,z_1 z_2 (z_1^5 + z_1^4 z_2 + \dots + z_1 z_2^4 + z_2^5) + \dots$$

Wir setzen $w = \lambda\,z + \mu$ in die Gleichung für E ein und erhalten eine Gleichung dritten Grades in z:

$$(1 + A\,\lambda^2 + B\,\lambda^3) z^3 + \lambda\mu(2A + 3B\lambda) z^2 + (\dots) z + (\dots) = 0$$

Wir kennen bereits zwei Lösungen $z = z_1, z_2$ dieser Gleichung. Für die dritte gilt dann

$$\begin{aligned} -z_3 &= \lambda\mu\frac{2A + 3B\lambda}{1 + A\,\lambda^2 + B\,\lambda^3} + z_1 + z_2 \\ &= z_1 + z_2 - 2A\,z_1z_2(z_1^3 + 2z_1^2z_2 + 2z_1z_2^2 + z_2^3) \\ &\quad - 3B\,z_1z_2(z_1^5 + 3z_1^4z_2 + 5z_1^3z_2^2 + 5z_1^2z_2^3 + 3z_1z_2^4 + z_2^5) + \dots \\ &=: F_E(z_1, z_2)\,. \end{aligned}$$

Da $-z_3$ die z-Koordinate von $P_1 + P_2$ ist, gilt also

$$z(P_1 + P_2) = F_E(z_1, z_2)\,.$$

Aus der Gruppenstruktur von E ergeben sich nun für $F = F_E$ folgende Eigenschaften, wobei $i(z) = -z$:

$$\begin{aligned} F(z, 0) = F(0, z) &= z \\ F(z_1, z_2) &= F(z_2, z_1) \\ F(z, i(z)) = F(i(z), z) &= 0 \\ F(F(z_1, z_2), z_3) &= F(z_1, F(z_2, z_3)) \end{aligned}$$

Definition 4.40. Eine Potenzreihe $F \in R[\![z_1, z_2]\!]$ mit obigen Eigenschaften (wobei $i \in R[\![z]\!]$ eine geeignete Potenzreihe ist) heißt eine *(einparametrige, kommutative) formale Gruppe* über R.

Beispiele für formale Gruppen (neben der formalen Gruppe F_E der elliptischen Kurve E) sind die additive formale Gruppe $F_{\mathrm{a}}(z_1, z_2) = z_1 + z_2$ und die multiplikative formale Gruppe $F_{\mathrm{m}}(z_1, z_2) = z_1 + z_2 + z_1z_2$ (da 0 die Rolle des neutralen Elementes spielt, ist die übliche Multiplikation um 1 verschoben: $1 + F_{\mathrm{m}}(z_1, z_2) = (1 + z_1)(1 + z_2)$).

Man kann sich eine formale Gruppe vorstellen als eine „Gruppenverknüpfung ohne Elemente“ oder als eine „Gruppe ohne unterliegende Menge“. Wie man aus einer formalen Gruppe eine echte Gruppe machen kann, werden wir noch sehen.

Zunächst müssen wir zu den formalen Gruppen die formalen Homomorphismen betrachten. In Analogie zur Verknüpfung ist so ein Homomorphismus durch eine Potenzreihe gegeben.

Definition 4.41. Seien F und G formale Gruppen über einem Ring R. Ein *formaler Homomorphismus* von F nach G ist eine Potenzreihe $f \in zR[\![z]\!]$, so daß $f(F(z_1, z_2)) = G(f(z_1), f(z_2))$.

Zum Beispiel haben wir für jeden Ring R, der $\mathbb{Q}$ enthält, die zu einander inversen Homomorphismen $\log(1 + z)$ und $\exp(z) - 1$ zwischen der additiven und der multiplikativen Gruppe. (Allgemeiner gilt für solche Ringe sogar, daß *jede* formale Gruppe zur additiven Gruppe isomorph ist, vergleiche [Si1, Ch. IV].)

Als spezielle Homomorphismen hat man wie in jeder abelschen Gruppe die Multiplikationsabbildungen.

DEFINITION 4.42. Sei F eine formale Gruppe über R. WIr definieren Homomorphismen $[m]$ von F nach F für jedes $m \in \mathbb{Z}$ durch

$$[0](z) = 0\,, \quad [m+1](z) = F([m](z), z) \quad [-m](z) = i([m](z))\,.$$

LEMMA 4.43. *Unter obigen Voraussetzungen gilt* $[m](z) = (m \cdot 1_R)\, z + O(z^2)$.

BEWEIS: Aus $F(z,0) = F(0,z) = z$ folgt $F(z_1, z_2) = z_1 + z_2 + O(z_1 z_2)$, und aus $F(z, i(z)) = 0$ folgt $i(z) = -z + O(z^2)$. Der Beweis erfolgt nun leicht durch Induktion aus der Definition von $[m]$. □

6.2. Echte Gruppen aus formalen Gruppen. Wie kann man nun aus einer formalen Gruppe eine richtige Gruppe gewinnen? Dazu braucht man eine geeignete unterliegende Menge, deren Elemente man in die verschiedenen Potenzreihen einsetzen kann. Man könnte z.B. daran denken, reelle oder komplexe Zahlen zu verwenden. Dann hat man aber das Problem, daß der Konvergenzbereich von F normalerweise nicht unter Einsetzen in F abgeschlossen ist, d.h. es kann vorkommen, daß zwar z_1 und z_2 im Konvergenzbereich liegen, $F(z_1, z_2)$ aber nicht mehr. Ein besseres Verhalten ergibt sich für nicht-archimedische Metriken, wie zum Beispiel bei den p-adischen Zahlen. Sei also etwas allgemeiner R ein *vollständiger lokaler Ring*, das ist ein Ring mit genau einem maximalen Ideal $\mathfrak{m}$ („lokal“), so daß $R \cong \varprojlim R/\mathfrak{m}^n$ („vollständig“). Wieder sind $\mathbb{Z}_p$ und $k[\![X]\!]$ Beispiele. Wenn F eine Potenzreihe (in evtl. mehreren Variablen) mit Koeffizienten in R ist, dann konvergiert $F(z_1, \ldots, z_n)$, sobald die $z_j \in \mathfrak{m}$ sind. Dies nutzt man aus, um eine Gruppe zu bekommen.

DEFINITION 4.44. Sei R ein vollständiger lokaler Ring mit maximalem Ideal $\mathfrak{m}$ und F eine formale Gruppe über R. Für $n \geq 1$ sei $F(\mathfrak{m}^n)$ die Gruppe mit unterliegender Menge $\mathfrak{m}^n$ und Gruppenverknüpfung gegeben durch Einsetzen in F. Wir schreiben $x +_F y$ und $[m]_F x$ für die Addition und Vervielfachung in dieser Gruppe.

Da F kein konstantes Glied hat, ist $\mathfrak{m}^n$ unter der Verknüpfung abgeschlossen. Daß $\mathfrak{m}^n$ mit dieser Verknüpfung eine Gruppe wird, folgt aus den Eigenschaften von F durch Einsetzen von Elementen.

Zum Beispiel ist $F_{\mathrm{a}}(\mathfrak{m}^n)$ die additive Gruppe $\mathfrak{m}^n$, während $F_{\mathrm{m}}(\mathfrak{m}^n)$ isomorph zu der multiplikativen Gruppe $1 + \mathfrak{m}^n$ der „Einseinheiten n-ter Stufe“ ist.

LEMMA 4.45. *Sei R ein vollständiger lokaler Ring mit maximalem Ideal $\mathfrak{m}$ und F eine formale Gruppe über R. Für $m \in \mathbb{Z}$ und $x \in \mathfrak{m}^n$ gilt dann:*

(1) $[m]_F x \in \mathfrak{m}^n$.
(2) *Wenn $m \cdot 1_R \in \mathfrak{m}$ ist, dann gilt $[m]_F x \in \mathfrak{m}^{n+1}$.*

BEWEIS: Teil (1) ergibt sich daraus, daß $F(\mathfrak{m}^n)$ eine Gruppe ist. Für Teil (2) sei $m \cdot 1_R \in \mathfrak{m}$. Es gilt $[m](z) = (m \cdot 1_R)z + O(z^2)$, also

$$[m]_F x = [m](x) = (m \cdot 1_R)x + O(x^2) \in \mathfrak{m}^{n+1} + \mathfrak{m}^{2n} = \mathfrak{m}^{n+1}\,.$$

□

6.3. Beweis des Lemmas. Jetzt können wir Lemma 4.35 beweisen. Dazu müssen wir uns noch überlegen, was der Zusammenhang zwischen der formalen Gruppe und Punkten $P \in E$ mit $v_\mathfrak{p}(x) < 0$ ist.

LEMMA 4.46. *Sei K ein Zahlkörper und $\mathfrak{p}$ ein Primideal von $\mathcal{O}_K$. Sei $K_\mathfrak{p}$ die Komplettierung von K bei $\mathfrak{p}$ (d.h. $K_\mathfrak{p}$ ist der Quotientenkörper des vollständigen lokalen Rings $\mathcal{O}_{K,\mathfrak{p}} = \varprojlim \mathcal{O}_K/\mathfrak{p}^n$; vergleiche $\mathbb{Z}_p$ und $\mathbb{Q}_p$). Sei weiter $E : y^2 = x^3 + A\,x + B$ eine elliptische Kurve über K mit Koeffizienten $A, B \in \mathcal{O}_K$. Sei außerdem*

$$E^1(K_\mathfrak{p}) = \{(\xi, \eta) \in E(K_\mathfrak{p}) \mid v_\mathfrak{p}(\xi) < 0\} \cup \{O\}$$

und F_E die formale Gruppe von E. Dann haben wir einen Isomorphismus

$$E^1(K_\mathfrak{p}) \ni P \longmapsto z(P) = x(P)/y(P) \in F_E(\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}})\,.$$

Für $P \in E^1(K_\mathfrak{p})$ gilt dann außerdem $v_\mathfrak{p}(x(P)) = -2v_\mathfrak{p}(z(P))$.

BEWEIS: Aus der Gleichung von E folgt erst einmal (wir schreiben kurz v statt $v_\mathfrak{p}$) für alle $P \in E(K_\mathfrak{p})$

$$v(x(P)) < 0 \iff v(y(P)) < 0 \iff \exists n > 0 : v(x(P)) = -2n, v(y(P)) = -3n\,.$$

Aus der Gleichung $w = z^3 + A\,w^2 z + B\,w^3$ folgt in ähnlicher Weise durch Vergleich der Bewertungen der Terme

$$v(z(P)) > 0 \iff v(w(P)) > 0 \iff \exists n > 0 : v(z(P)) = n, v(w(P)) = 3n\,.$$

Aus beidem zusammen folgt $v(x(P)) < 0 \iff v(z(P)) > 0$, und dann ist $v(x(P)) = -2v(z(P))$. Das zeigt schon einmal, daß eine Bijektion vom Mengen vorliegt (die inverse Abbildung ist durch $z \mapsto (x(z), y(z))$ gegeben). Daß die Abbildung auch ein Gruppenhomomorphismus ist, ergibt sich aus der Konstruktion von F_E und der Definition von $F_E(\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}})$. □

Der Beweis von Lemma 4.35 ergibt sich nun sofort, wenn man Lemma 4.45 und Lemma 4.46 miteinander kombiniert.

7. Höhen

Um den Beweis des Satzes von Mordell-Weil abzuschließen, müssen wir noch die Existenz einer Höhenfunktion auf $E(K)$ nachweisen. Dazu betrachten wir erst einmal allgemeiner die Theorie der Höhe auf projektiven Räumen.

7.1. Höhen auf dem projektiven Raum. In Analogie zur projektiven Ebene $\mathbb{P}^2$ gilt für den n-dimensionalen projektiven Raum $\mathbb{P}^n$, daß die Menge seiner K-rationalen Punkte gegeben ist durch

$$\mathbb{P}^n(K) = (K^{n+1} \setminus \{0\})/K^\times\,,$$

wobei $K^\times$ durch komponentenweise Multiplikation operiert. Sei K ein Zahlkörper. Wir wollen eine Funktion $H_K : \mathbb{P}^n(K) \to \mathbb{R}_{\geq 1}$ definieren, die in gewisser Weise die Kompliziertheit der Punkte mißt. Im Fall $K = \mathbb{Q}$ ist folgende Definition naheliegend. Ein Punkt $P \in \mathbb{P}^n(\mathbb{Q})$ hat eine (bis auf gemeinsames Vorzeichen eindeutige) Darstellung mit ganzzahligen, relativ primen Koordinaten $P = (x_0 : \cdots : x_n)$; man setzt dann $H(P) = \max\{|x_0|, \ldots, |x_n|\}$.

Diese Definition läßt sich aber nicht so ohne weiteres auf Zahlkörper K verallgemeinern — man kann natürlich immer noch ganz-algebraische Koordinaten wählen, aber der größte gemeinsame Teiler kann im allgemeinen ein Ideal sein, das kein Hauptideal ist, so daß man ihn nicht herausdividieren kann. Um diese Schwierigkeit zu umgehen, brauchen wir etwas Zahlentheorie.

DEFINITION 4.47. Sei K ein Zahlkörper. Eine *Stelle* von K ist eines der folgenden Objekte.

(i) Ein Primideal $\mathfrak{p} \subset \mathcal{O}_K$.
(ii) Eine Einbettung $\sigma : K \to \mathbb{R}$.
(iii) Ein Paar $\sigma, \bar{\sigma}$ von konjugiert komplexen Einbettungen $K \to \mathbb{C}$ (mit $\sigma(K) \not\subset \mathbb{R}$).

Die Menge aller Stellen von K wird mit M_K bezeichnet.

Ist $v \in M_K$, dann ist der zugehörige *normierte Absolutbetrag* $K \ni x \mapsto |x|_v$ definiert durch

(i) $|x|_v = (\mathrm{N}\mathfrak{p})^{-v_\mathfrak{p}(x)}$,
(ii) $|x|_v = |\sigma(x)|$,
(iii) $|x|_v = |\sigma(x)|^2 = |\bar{\sigma}(x)|^2$.

($\mathrm{N}\mathfrak{p} = \#\mathcal{O}_K/\mathfrak{p}$ ist die absolute Norm von $\mathfrak{p}$.) In den drei Fällen setzen wir $\varepsilon_v = 0, 1, 2$. Dann gilt die Dreiecksungleichung

$$|x_1 + x_2 + \cdots + x_n|_v \le n^{\varepsilon_v} \max\{|x_1|_v, |x_2|_v, \ldots, |x_n|_v\}\,.$$

Außerdem gilt $|x|_v \ge 0$, $|x|_v = 0 \iff x = 0$, $|xy|_v = |x|_v|y|_v$.

Ist $K \subset L$ eine Erweiterung von Zahlkörpern, und sind $v \in M_K$, $w \in M_L$, dann schreiben wir $w \mid v$ („w liegt über v“), wenn entweder beide Male Fall (i) vorliegt und $\mathfrak{p}_w \cap \mathcal{O}_K = \mathfrak{p}_v$ gilt oder wenn beide Male die Fälle (ii) oder (iii) vorliegen und sich die Einbettung(en) von K durch Einschränkung der Einbettung(en) von L ergeben.

Die wichtigste Eigenschaft dieser Absolutbeträge ist die folgende *Produktformel*:

$$\text{Für alle } 0 \ne x \in K \text{ gilt} \qquad \prod_{v \in M_K} |x|_v = 1\,.$$

Für $K = \mathbb{Q}$ ist das leicht zu sehen (wegen Multiplikativität reicht es, $x = -1$ und $x = p$ prim zu betrachten); für beliebiges K führt man es auf den Fall $K = \mathbb{Q}$ zurück, indem man folgende Eigenschaft benutzt.

LEMMA 4.48. *Sei $K \subset L$ eine Erweiterung von Zahlkörpern. Dann gilt für alle $x \in L$*

$$\prod_{w \in M_L, w \mid v} |x|_w = |N_{L/K}(x)|_v\,.$$

Damit definieren wir nun die Höhe auf $\mathbb{P}^n$.

DEFINITION 4.49. Für einen Zahlkörper K ist die *Höhe* auf $\mathbb{P}^n$ definiert durch

$$H_K((x_0 : x_1 : \cdots : x_n)) = \prod_{v \in M_K} \max\{|x_0|_v, |x_1|_v, \ldots, |x_n|_v\}\,.$$

Die *logarithmische Höhe* ist $h_K(P) = \log H_K(P)$.

Auf Grund der Produktformel ist die Höhe wohldefiniert, denn sie hängt nicht von der Skalierung der Koordinaten ab. Im Fall von $K = \mathbb{Q}$ stimmt diese Definition mit der „naiven“ oben überein, denn bei teilerfremden ganzzahligen Koordinaten trägt nur der Term mit dem gewöhnlichen Absolutbetrag etwas bei.

Da wir stets ein $x_j = 1$ wählen können, gilt stets $H_K(P) \geq 1$ (bzw. $h_K(P) \geq 0$). Außerdem gilt (das werden wir aber im Folgenden nicht brauchen) für Zahlkörper $K \subset L$ und $P \in \mathbb{P}^n(K)$, daß $H_L(P) = H_K(P)^{[L:K]}$ bzw. $h_L(P) = [L : K]h_K(P)$. Daher kann man eine *absolute Höhe* auf $\mathbb{P}^n(\bar{\mathbb{Q}})$ definieren durch $H(P) = H_K(P)^{1/[K:\mathbb{Q}]}$, wenn $P \in \mathbb{P}^n(K)$ ist.

Für uns wird wichtig sein, wie sich die Höhe unter Morphismen zwischen projektiven Räumen verhält. Morphismen haben wir schon kennengelernt im Spezialfall $\mathbb{P}^2 \to \mathbb{P}^2$. Die allgemeine Definition ist völlig analog.

Definition 4.50. Ein über K definierter *Morphismus F vom Grad d* von $\mathbb{P}^n$ nach $\mathbb{P}^m$ ist gegeben durch ein Tupel von homogenen Polynomen vom Grad d: $F_0, \ldots, F_m \in K[X_0, \ldots, X_n]$, die außer 0 keine gemeinsame Nullstelle haben. Damit bekommen wir eine Abbildung

$$F : \mathbb{P}^n(K) \ni (x_0 : \cdots : x_n) \longmapsto (F_0(x_0, \ldots, x_n) : \cdots : F_m(x_0, \ldots, x_n)) \in \mathbb{P}^m(K)\,.$$

Das Hauptresultat über Höhen ist nun das folgende.

Satz 4.51. *Sei F ein über K definierter Morphismus $\mathbb{P}^n \to \mathbb{P}^m$ vom Grad d. Dann gibt es Konstanten $C_1, C_2 > 0$, so daß für alle $P \in \mathbb{P}^n(K)$ gilt*

$$C_1 H_K(P)^d \leq H_K(F(P)) \leq C_2 H_K(P)^d\,.$$

Beweis: Sei $v \in M_K$. Wir setzen $|F|_v$ gleich dem Maximum der $|c|_v$, wo c alle Koeffizienten von allen F_j durchläuft. Wir wählen Koordinaten für $P = (x_0 : \cdots : x_n)$ und setzen analog $|P|_v = \max_i |x_i|_v$ und $|F(P)|_v = \max_j |F_j(x)|_v$. Sei weiter N die maximale Anzahl der Terme in einem der F_j. Aus der Dreiecksungleichung folgt dann

$$|F(P)|_v \leq N^{\varepsilon_v} |F|_v |P|_v^d\,.$$

Wir setzen noch $H_K(F) = \prod_v |F|_v$ (wohldefiniert, da für fast alle v gilt $|F|_v = 1$). Dann folgt durch Multplikation über alle v (und unter Beachtung von $\sum_v \varepsilon_v = [K : \mathbb{Q}]$)

$$H_K(F(P)) = \prod_{v \in M_K} |F(P)|_v \leq \prod_{v \in M_K} N^{\varepsilon_v} |F|_v |P|_v^d = N^{[K:\mathbb{Q}]} H_K(F) H_K(P)^d\,.$$

Damit ist die zweite Ungleichung gezeigt.

Um die erste Ungleichung zu zeigen, müssen wir verwenden, daß F ein Morphismus ist, daß also die Komponenten F_j keine nichttriviale gemeinsame Nullstelle haben. In diesem Fall folgt aus dem Hilbertschen Nullstellensatz (siehe Bücher über kommutative Algebra oder algebraische Geometrie), daß es $e > 0$ gibt und homogene Polynome G_{ij} vom Grad $e - d$, so daß

$$X_i^e = \sum_j G_{ij} F_j\,.$$

Wir definieren $|G|_v$ analog zu $|F|_v$ als das Maximum aller $|c|_v$, wo c ein Koeffizient eines der G_{ij} ist und $H_K(G) = \prod_v |G|_v$. Außerdem sei M die Maximalzahl von Termen in einem der G_{ij}. Wie oben schließen wir nach Einsetzen von P

$$|P|_v^e = \max_i |\sum_j G_{ij}(x)F_j(x)|_v \le M^{\varepsilon_v}|G|_v|P|_v^{e-d}|F(P)|_v\,.$$

Wir multiplizieren das mit $|P|_v^{d-e}$ und bilden dann das Produkt über alle v:

$$H_K(P)^d = \prod_{v\in M_K} |P|_v^d \le \prod_{v\in M_K} M^{\varepsilon_v}|G|_v|F(P)|_v = M^{[K:\mathbb{Q}]}H_K(G)H_K(F(P))\,.$$

Damit ist auch die erste Ungleichung bewiesen. □

Wir brauchen noch eine weitere ähnliche Aussage.

LEMMA 4.52. *Sei* $\varphi_n : \mathbb{P}^1 \times \mathbb{P}^n \longrightarrow \mathbb{P}^{n+1}$ *gegeben durch*

$$\begin{aligned}\varphi_n((x_0 : x_1),&(y_0 : y_1 : \ldots : y_n))\\ &= (x_0y_0 : x_1y_0 + x_0y_1 : x_1y_1 + x_0y_2 : \ldots : x_1y_{n-1} + x_0y_n : x_1y_n)\,.\end{aligned}$$

Dann gilt für $P \in \mathbb{P}^1(K)$, $Q \in \mathbb{P}^n(K)$*:*

$$(n+1)^{-[K:\mathbb{Q}]}H_K(P)H_K(Q) \le H_K(\varphi_n(P,Q)) \le 2^{[K:\mathbb{Q}]}H_K(P)H_K(Q)\,.$$

BEWEIS: Wir benutzen die Bezeichnungen $|P|_v$, $|Q|_v$, $|\varphi_n(P,Q)|_v$ wie im vorigen Beweis. Die rechte Ungleichung folgt leicht aus

$$|\varphi_n(P,Q)|_v \le 2^{\varepsilon_v}|P|_v|Q|_v\,.$$

Für die linke Ungleichung gehen wir wieder so vor wie im letzten Beweis. Explizit haben wir

$$\begin{aligned}x_0^{n+1}y_k &= \sum_{j=0}^{k-1}(-1)^j x_0^{n-j}x_1^j(x_0y_{k-j} + x_1y_{k-j-1}) + (-1)^k x_0^{n-k}x_1^k\cdot(x_0y_0)\,,\\ x_1^{n+1}y_k &= \sum_{j=0}^{n-k-1}(-1)^j x_0^j x_1^{n-j}(x_0y_{k+j+1} + x_1y_{k+j}) + (-1)^{n-k}x_0^{n-k}x_1^k\cdot(x_1y_n)\,.\end{aligned}$$

Daraus ergibt sich

$$|P|_v^{n+1}|Q|_v \le (n+1)^{\varepsilon_v}|P|_v^n|\varphi_n(P,Q)|_v\,,$$

woraus dann die linke Ungleichung in der üblichen Weise folgt. □

Wenn wir das iterieren, erhalten wir folgendes Resultat.

PROPOSITION 4.53. *Sei* $\phi_n : (\mathbb{P}^1)^n \longrightarrow \mathbb{P}^n$ *folgender Morphismus.*

$$\begin{aligned}\phi_n((x_1 : y_1),&(x_2 : y_2),\ldots,(x_n : y_n))\\ &= (x_1x_2\ldots x_n : y_1x_2\ldots x_n + \cdots + x_1\ldots x_{n-1}y_n\\ &\qquad : y_1y_2x_3\ldots x_n + y_1x_2y_3x_4\ldots x_n + \cdots : \ldots : y_1y_2\ldots y_n)\,.\end{aligned}$$

(D.h. wir betrachten die Koeffizienten von $\prod(x_jX + y_j)$*.)*

Dann gilt für $P_1,\ldots,P_n \in \mathbb{P}^1(K)$*, daß*

$$(n!)^{-[K:\mathbb{Q}]}H_K(P_1)\ldots H_K(P_n) \le H_K(\phi_n(P_1,\ldots,P_n)) \le 2^{(n-1)[K:\mathbb{Q}]}H_K(P_1)\ldots H_K(P_n)\,.$$

BEWEIS: Es ist $\phi_n(P_1,\dots,P_n) = \varphi_{n-1}(\dots\varphi_2(\varphi_1(P_1,P_2),P_3)\dots,P_n)$. Die Behauptung folgt dann aus dem vorstehenden Lemma. □

Die Konstante $n!$ läßt sich verbessern, vergleiche [Si1, Thm. VIII.5.9].

Wir können jetzt eine weitere wichtige Eigenschaft der Höhe folgern.

SATZ 4.54. *Sei K ein Zahlkörper und $C > 0$. Dann ist die Menge der Punkte $P \in \mathbb{P}^n(K)$ mit $H_K(P) \le C$ endlich.*

BEWEIS: Es genügt, sich auf ein affines Teilstück des $\mathbb{P}^n$ zu beschränken (der Rest ist ein $\mathbb{P}^{n-1}$ oder wird von endlich vielen anderen affinen Teilstücken überdeckt). Wir setzen also $x_0 = 1$. Dann gilt $\max\{1,|x_j|_v\} \le \max\{1,|x_1|_v,\dots,|x_n|_v\}$, also $H_K((1:x_j)) \le H_K(P)$. Es genügt also zu zeigen, daß die Menge aller $x \in K$ mit $H_K(x) := H_K((1:x)) \le C$ endlich ist.

Um das zu zeigen, können wir ohne Einschränkung annehmen, daß $K/\mathbb{Q}$ Galoissch ist (sonst betrachte den Galoisschen Abschluß L von K und ersetze C durch $C^{[L:K]}$). In diesem Fall gilt für $x \in K$ und $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, daß $|x^\sigma|_{v^\sigma} = |x|_v$, also folgt $H_K(x^\sigma) = H_K(x)$. Wir betrachten nun das charakteristische Polynom $F = \prod_\sigma (X - x^\sigma)$. Es hat Koeffizienten in $\mathbb{Q}$, und nach Prop. 4.53 gilt $H_{\mathbb{Q}}(F) \le [K:\mathbb{Q}]! H_K(x)$ (nach Ziehen der $[K:\mathbb{Q}]$-ten Wurzel und Identifikation von F mit dem durch seine Koeffizienten gegebenen Punkt in $\mathbb{P}^{[K:\mathbb{Q}]}(\mathbb{Q})$).

Es genügt also zu zeigen, daß $\{P \in \mathbb{P}^n(\mathbb{Q}) \mid H(P) \le C'\}$ endlich ist. Das ist aber elementar (benutze die naive Definition der Höhe). □

7.2. Anwendung auf elliptische Kurven. Wir wollen die bisher entwickelte Theorie der Höhe nun auf elliptische Kurven anwenden. Dazu definieren wir die Höhe eines Punktes wie folgt.

DEFINITION 4.55. Sei E/K eine elliptische Kurve über einem Zahlkörper, gegeben durch eine Weierstraßgleichung. Für $P \in E(K)$ sei $h_K(P) = h_K(x(P))$ die (logarithmische) *Höhe* von P. (Dabei ist $x : E \to \mathbb{P}^1, (x:y:z) \mapsto (x:z)$ der x-Koordinaten-Morphismus.)

Zwei der für den Beweis des Satzes von Mordell-Weil benötigten Eigenschaften folgen aus folgendem Satz.

SATZ 4.56. *Sei E/K eine elliptische Kurve über einem Zahlkörper, gegeben durch eine kurze Weierstraßgleichung $y^2 = x^3 + Ax + B$. Dann gibt es $C > 0$, so daß für alle $P, Q \in E(K)$ gilt*

$$|h_K(P+Q) + h_K(P-Q) - 2\,h_K(P) - 2\,h_K(Q)| \le C\,.$$

BEWEIS: Sei $\psi : \mathbb{P}^2 \to \mathbb{P}^2$ gegeben durch

$$\psi(t:u:v) = (u^2 - 4tv : 2u(At+v) + 4Bt^2 : (v-At)^2 - 4Btu)\,.$$

Dann ist ψ ein Morphismus. (Denn $t = 0$ führt sofort auf $u = v = 0$, so daß man $t = 1$ annehmen kann. Dann ist $v = u^2/4$, und man sieht, daß die zwei Polynome in u, die man durch Einsetzen erhält, keine gemeinsame Nullstelle haben, wenn $\Delta_E \ne 0$ ist [ggT-Berechnung].) Wir setzen außerdem $\Psi : E \times E \to E \times E$,

$\Psi(P,Q) = (P+Q, P-Q)$. Dann kann man nachrechnen, daß folgendes Diagramm kommutiert.

$$\begin{array}{ccc} E \times E & \xrightarrow{\Psi} & E \times E \\ {\scriptstyle (x,x)}\downarrow & & \downarrow{\scriptstyle (x,x)} \\ \mathbb{P}^1 \times \mathbb{P}^1 & & \mathbb{P}^1 \times \mathbb{P}^1 \\ {\scriptstyle \phi_2}\downarrow & & \downarrow{\scriptstyle \phi_2} \\ \mathbb{P}^2 & \xrightarrow{\psi} & \mathbb{P}^2 \end{array}$$

Wir schreiben im Folgenden $f = g + O(1)$, wenn die Differenz $f - g$ beschränkt ist. Nach Satz 4.51 und Prop. 4.53 gilt (nach Logarithmieren)

$$\begin{aligned} h_K(P+Q) + h_K(P-Q) &= h_K(\phi_2(x(P+Q), x(P-Q))) + O(1) \\ &= 2h_K(\phi_2(x(P), x(Q))) + O(1) \\ &= 2(h_K(P) + h_K(Q)) + O(1)\,. \end{aligned}$$

Das ist die Behauptung. □

Nun sind wir fertig:

PROPOSITION 4.57. *Die Funktion $h_K : E(K) \to \mathbb{R}_{\geq 0}$ hat folgende Eigenschaften.*

(i) *Für jedes C ist die Menge $\{P \in E(K) \mid h_K(P) \leq C\}$ endlich.*
(ii) *Für jeden Punkt $Q \in E(K)$ gibt es eine Konstante $c(Q)$, so daß für alle $P \in E(K)$ gilt:*
$$h_K(P+Q) \leq 2\, h_K(P) + c(Q)\,.$$
(iii) *Für jedes $m \geq 2$, gibt es eine Konstante c_m, so daß für alle $P \in E(K)$ gilt:*
$$h_K(mP) \geq m^2\, h_K(P) - c_m\,.$$

BEWEIS: (i) Nach Satz 4.54 gibt es nur endlich viele $x \in \mathbb{P}^1(K)$ mit $h_K(x) \leq C$. Da es zu jedem $x \in \mathbb{P}^1(K)$ höchstens zwei Punkte $P \in E(K)$ gibt mit $x(P) = x$, ist auch die in Frage stehende Menge endlich.

(ii) Es gilt $h_K(P+Q) \leq h_K(P+Q) + h_K(P-Q) = 2h_K(P) + 2h_K(Q) + O(1)$, woraus sich die Behauptung unmittelbar ergibt.

(iii) Durch Induktion erhalten wir aus Satz 4.56, daß $h_K(mP) = m^2\, h_K(P) + O(1)$. Das impliziert die Behauptung. □

Literaturverzeichnis

[Bro] K.S. Brown: *Cohomology of groups*, Springer GTM **87** (1982).

[Cas] J.W.S. Cassels: *Lectures on elliptic curves*, London Mathematical Society Student Texts **24**, Cambridge University Press (1991).

[CF] J.W.S. Cassels, A. Fröhlich (eds): *Algebraic Number Theory*, Academic Press (second printing 1969).

[Hus] D. Husemöller: *Elliptic curves*, Springer GTM **111** (1987).

[Jae] K. Jänich: *Einführung in die Funktionentheorie*, Springer Hochschultext (2. Auflage 1980).

[Kna] A.W. Knapp: *Elliptic curves*, Mathematical Notes **40**, Princeton University Press (1992).

[Neu] J. Neukirch: *Algebraische Zahlentheorie*, Springer (1992).

[Si1] J.H. Silverman: *The arithmetic of elliptic curves*, Springer GTM **106** (1986).

[Si2] J.H. Silverman: *Advanced topics in the arithmetic of elliptic curves*, Springer GTM **151** (1994).