Das Schwache Mordell-Weil-Theorem und die Abstiegsmethode

Vortrag 10

Gregor Pohl

2.7.2015

0 Einleitung

Das übergreifende Ziel der letzten drei Vorträge des Seminars ist der Beweis des Mordell-Weil-Theorems:

Theorem 0.1 (Mordell-Weil)**.** *Sei K ein Zahlkörper, E/K eine elliptische Kurve. Dann ist $E(K)$ eine endlich erzeugte abelsche Gruppe.*

Hierzu wird zunächst das schwache Mordell-Weil Theorem bewiesen:

Theorem 0.2 (schwaches Mordell-Weil)**.** *Sei K ein Zahlkörper, E/K eine elliptische Kurve, und $m \in \mathbb{N}$. Dann ist $E(K)/m$ eine endliche abelsche Gruppe.*

Danach wird mit der sogenannten Abstiegsmethode das vollständige Theorem gefolgert. Beide Schritte werden hier vorgestellt; in den letzten beiden Vorträgen werden dann hauptsächlich die für die Abstiegsmethode notwendigen Voraussetzungen überprüft (Es muss eine Höhenfunktion gefunden werden).

Wir richten uns im Folgenden nach Kapitel VIII, §1-4 des Buches „The Arithmetic of Elliptic Curves“ von Joseph H. Silverman.

1 Das schwache Mordell-Weil-Theorem

Im gesamten Abschnitt sei K ein Zahlkörper, M_K (bzw. M_K^0, M_K^∞) die Menge der (nicht-archimedischen, archimedischen) Primstellen (d.h. Bewertungen) von K, E/K eine elliptische Kurve, und $m > 0$ eine natürliche Zahl.

Der Beweis des schwachen Mordell-Weil-Theorems erfolgt über Kummer-Theorie, welche sich am schönsten in kohomologischer Sprache ausdrücken lässt. Um ein Gefühl für diese Methode zu vermitteln, werden wir zumindest das erste Lemma kohomologisch beweisen.

Definition 1.1 (Galoiskohomologie)**.** Sei G eine Gruppe.

i) Ein G-(Links-)Modul A ist eine abelsche Gruppe zusammen mit einer kompatiblen G-(Links-)Wirkung, d.h. $g(a+b) = ga + gb \ \forall g \in G,\ a, b \in A$

ii) Ein Homomorphismus von G-Moduln ist ein G-äquivarianter Homomorphismus abelscher Gruppen. Hierdurch wird die Kategorie G-Mod der G-Linksmoduln zu einer abelschen Kategorie.

iii) Die Invariantenuntergruppe A^G von A ist die Untergruppe der unter der G-Wirkung invarianten Elemente von A. Man sieht leicht, dass dies ein linksexakter Funktor ist.

iv) $\mathrm{H}^i(G, A) := R^i(-^G)(A)$ heisst die i-te Kohomologiegruppe von G mit Koeffizienten in A.

Die Kohomologiegruppen lassen sich über eine Auflösung bestimmen, welche aus Gruppen der Form $\mathrm{Abb}(G^n, A)$ besteht. Hieraus ergibt sich unmittelbar das folgende

Lemma 1.2. *Sind G und A endlich, so auch $\mathrm{H}^i(G, A)$ für alle $i \in \mathbb{N}$.*

Wir sind nun bereit, das folgende Reduktionslemma zu beweisen.

Lemma 1.3. *Ist L/K eine endliche Galoiserweiterung, und ist $E(L)/m$ endlich, so ist auch $E(K)/m$ endlich.*

Beweis. Sei $G_{L/K}$ die Galoisgruppe. Betrachte die kurze exakte Folge von $G_{L/K}$-Moduln

$$0 \to E[m](L) \to E(L) \xrightarrow{m} mE(L) \to 0.$$

Durch Anwendung von $-^G$ erhalten wir

$$0 \to E[m](K) \to E(K) \xrightarrow{m} mE(L) \cap E(K) \to \mathrm{H}^1(G_{L/K}, E[m](L)),$$

und somit eine Injektion $\Phi := \frac{mE(L)\cap E(K)}{mE(K)} \hookrightarrow \mathrm{H}^1(G_{L/K}, E[m](L))$. $G_{L/K}$ und $E[m](L)$ sind endlich, wegen Lemma 1.2 ist Φ also endlich. Φ ist aber gerade der Kern des Homomorphismus $E(K)/m \to E(L)/m$, welcher nach Voraussetzung auch endliches Bild hat. Somit ist $E(K)/m$ ebenfalls endlich. □

Bemerkung 1.4. Die kurze exakte Folge in obigem Beweis heißt die *Kummer-Folge für elliptische Kurven*, und *Kummer-Theorie für elliptische Kurven* lässt sich als Betrachtung der assoziierten langen exakten Kohomologiefolge zusammenfassen. Die klassische Kummer-Theorie für Körper ergibt sich aus der analogen Folge $0 \to \mu_m(L) \to L^\times \xrightarrow{.^m} L^{\times m} \to 0$.

Wir erinnern uns an folgende Definition:

Definition 1.5. Ist $P \in E(K^{sep})$, wobei K^{sep} der separable Abschluss ist, so ist $K(P)$ die minimale Erweiterung von K über der P definiert ist, d.h. $K(P) = (K^{sep})^{G_{K,P}}$, wobei $G_K = Gal(K^{sep}/K)$, und $G_{K,P}$ den Stabilisator von P in G_K bezeichnet. $K(P)/K$ ist stets eine endliche Erweiterung.

Wegen Lemma 1.3 gehen wir im Folgenden o.B.d.A. davon aus, dass $E[m] \subset E(K)$.

Die folgende Definition wird es uns erlauben, das schwache Mordell-Weil-Theorem auf eine rein körpertheoretische Aussage zu reduzieren.

Definition 1.6 (Kummer-Paarung)**.** Sei $G_K = Gal(K^{sep}/K)$. Die Kummer Paarung κ ist definiert durch

$$\begin{aligned} \kappa : E(K) \times G_K &\to E[m] \\ (P, \sigma) &\mapsto \sigma(Q) - Q \end{aligned}$$

wobei $Q \in E(K^{sep})$, s.d. $[m]Q = P$.

Satz 1.7.

i) *κ ist wohldefiniert und $\kappa(\sigma, P)$ hängt nicht von der Wahl von Q ab.*

ii) *κ ist bilinear.*

iii) *Der Kern von κ links ist $mE(K)$.*

iv) *Der Kern von κ rechts ist G_L, wobei $L = K([m]^{-1}E(K))$ das Kompositum aller Körper $K(Q)$ mit $[m]Q \in E(K)$ ist.*

Somit induziert κ eine nichtentartete bilineare Paarung $E(K)/m \times G_{L/K} \to E[m]$.

Beweis. Wir beweisen beispielhaft nur *(iv)* und die letzte Aussage.

Sei $\sigma \in G_L$. Dann gilt $\kappa(P, \sigma) = \sigma(Q) - Q = O$, denn nach Definition von L ist Q über L definiert, und wird somit von σ fixiert.

Sei nun $\sigma \in G_K$ mit $\kappa(P, \sigma) = O$ für alle $P \in E(K)$. Dann gilt für alle $Q \in E(K^{sep})$ mit $[m]Q \in E(K)$ dass $\sigma(Q) - Q = \kappa([m]Q) = O$. Somit fixiert κ alle solchen Punkte Q, und somit auch L, nach der Definition von L. Folglich $\sigma \in G_L$.

Da nun $G_L = \ker(G_K \to \mathrm{Hom}(E(K), E[m]))$, ist G_L ein Normalteiler in G_K. Somit ist L/K galoissch, und aus *(i)-(iv)* folgt, dass wir durch herausteilen der Kerne auf beiden Seiten eine nichtentartete Paarung $\kappa : E(K)/m \times G_{L/K} \to E[m]$ erhalten. □

Im Folgenden ist L immer der in Satz 1.6 *(iv)* definierte Körper. Die Nichtentartetheit der Kummer-Paarung liefert eine Injektion $E(K)/m \hookrightarrow \mathrm{Hom}(G_{L/K}, E[m])$, und da $E[m]$ endlich ist, müssen wir für die Endlichkeit von $E(K)/m$ nur zeigen, dass L/K endlich ist. Wir untersuchen also die Eigenschaften von L.

Satz 1.8.

i) *L/K ist eine abelsche Erweiterung vom Exponent m, d.h. $G_{L/K}$ ist abelsch und die Ordnung jedes Elements teilt m.*

ii) *Sei $S = \{v \in M_K^0 | E \text{ hat schlechte Reduktion an } v\} \cup \{v \in M_K^0 | v(m) \neq 0\} \cup M_K^\infty$. Dann ist L/K unverzweigt ausserhalb von S.*

Beweis. (i) Folgt unmittelbar aus dem durch die Kummer-Paarung induzierten injektiven Gruppenhomomorphismus $G_{L/K} \hookrightarrow \mathrm{Hom}(E(K)/m, E[m])$, da $\mathrm{Hom}(E(K)/m, E[m])$ abelsch und vom Exponent m ist.

(ii) Sei $v \in M_K \backslash S$, $Q \in E(K^{sep})$ s.d. $[m]Q \in E(K)$, und sei $K' = K(Q)$. Da wir keine Einschränkungen an Q und v gestellt haben, reicht es zu zeigen, dass K'/K unverzweigt ist (denn Komposita unverzweigter Erweiterungen sind unverzweigt).

Sei $v' \in M_{K'}$ eine Stelle über v, und sei $k'_{v'}/k_v$ die Restklassenkörpererweiterung. Da E an v gute Reduktion hat, gilt dasselbe für v', denn wir können die selbe Weierstrass-Gleichung betrachten, und die Bedingungen an die Koeffizienten der Gleichung sind mit v' ebenfalls erfüllt. Somit haben wir die Reduktionsabbildung $E(K') \to \tilde{E}(k')$.

Sei nun $I_{v'/v} \subset G_{K'/K}$ die Trägheitsgruppe von v'/v, und sei $\sigma \in I_{v'/v}$. Nach Definition wirkt $I_{v'/v}$ trivial auf die reduzierte Kurve, somit gilt

$$\widetilde{Q^\sigma - Q} = \tilde{Q}^\sigma - \tilde{Q} = O.$$

Andererseits gilt auch

$$[m](Q^\sigma - Q) = ([m]Q)^\sigma - [m]Q = O,$$

denn $[m]Q \in E(K)$. Folglich liegt $Q^\sigma - Q \in E[m]$ im Kern der Reduktion-mod-v-Abbildung. Nach einem Satz des letzten Vortrages ist diese Abbildung aber injektiv auf den m-Torsionspunkten. Somit gilt $Q^\sigma - Q = O$, und da wir keine Einschränkungen an σ gestellt haben, wird Q von ganz $I_{v'/v}$ fixiert. somit ist K'/K unverzweigt an v, und es folgt die Unverzweigtheit von L/K ausserhalb S. □

Die in Satz 1.8 festgelegten Eigenschaften reichen schon aus, um die Endlichkeit von L/K zu folgern, wie der nächste Satz zeigt.

Satz 1.9. *Sei K ein Zahlkörper, S eine endliche Stellenmenge von K, $m \in \mathbb{N}$, und M/K die maximale abelsche Exponent-m-Erweiterung, die ausserhalb S unverzweigt ist. Dann ist M/K endlich.*

Zum Beweis von Satz 1.9 sei nur gesagt, dass er wieder über Kummertheorie verläuft, und dass zwei zahlentheoretische Sätze eingehen: die Endlichkeit der Idealklassengruppe, und die Endlich-Erzeugtheit der S-Einheitengruppe (der Dirichletsche S-Einheitensatz). Beide diese Sätze werden über analytische Methoden bewiesen, sind aber dennoch von grundlegender Bedeutung für die algebraische Zahlentheorie.

Beweis des schwachen Mordell-Weil-Theorems. Die in Satz 1.8 definierte Stellenmenge ist endlich, denn für eine Weierstrass-Gleichung mit Koeffizienten $a_1, .., a_6$ und Diskriminante Δ gilt $v(a_i) \geq 0$, $v(\Delta) = 0$ für fast alle v. Somit ist L in dem in Satz 1.9 definierten Körper M enthalten, also ist L/K endlich. Wie oben beschrieben folgt nun aus der Kummer-Paarung, dass auch $E(K)/m$ endlich ist. □

2 Die Abstiegsmethode

Das schwache Mordell-Weil-Theorem sagt uns, dass $E(K)/m$ für alle m endlich ist. Wir möchten nun zeigen, dass $E(K)$ auch endlich erzeugt ist. Das Hindernis hierbei scheint Teilbarkeit zu sein: In der Tat sind teilbare Gruppen nie endlich erzeugt, und die Faktorgruppen modulo m sind immer trivial. Um Teilbarkeit einzuschränken, wenden wir die sogenannte Abstiegsmethode an. Die Idee hierbei ist es, dass wir eine nach unten beschränkte Funktion (die Höhenfunktion) von $E(K)$ nach $\mathbb{R}$ finden, die stets sinkt wenn wir durch m teilen. Somit werden die m-teilbaren Elemente eingeschränkt. Im Anhang wird demonstriert, dass die Komplexität der x-Koordinate eines Punktes (bzgl. einer Weierstrass-Gleichung) in gekürzter Bruchdarstellung (scheinbar quadratisch) steigt, wenn man die Vielfachen des Punktes betrachtet. Diese Komplexität soll durch die Höhenfunktion erfasst werden.

Theorem 2.1 (Abstiegssatz)**.** *Sei A eine abelsche Gruppe, $h : A \to [0, \infty)$ eine Funktion, die folgenden Bedingungen genügt:*

i) *Sei $Q \in A$. Dann existiert $C_1^Q \in \mathbb{R}$, sodass*

$$h(P + Q) \leq 2h(P) + C_1^Q \ \forall Q \in A.$$

ii) *Es gibt eine ganze Zahl $m \geq 2$, und ein $C_2 \in \mathbb{R}$, sodass*

$$h(mP) \geq m^2 h(P) - C_2 \ \forall P \in A.$$

iii) *Für alle $S \in \mathbb{R}$ ist $\#\{P \in A | h(P) \leq S\} < \infty$.*

Ist weiterhin A/m endlich für das m aus (ii)*, dann ist A endlich erzeugt.*

Beweis. Wir können ohne Einschränkung $C_2 \geq 0$, $C_1^Q \geq 0 \ \forall Q \in A$ annehmen, denn wir können die Konstanten durch ihre Beträge ersetzen.

Seien nun $Q_1, .., Q_r$ Vertreter der endlich vielen Nebenklassen in A/m, und sei $P \in A$. Wir schreiben

$$P = mP_1 + Q_{i_1}$$

für ein $P_1 \in A$, $i_1 \in 1, .., r$. Induktiv definieren wir

$$\begin{aligned} P_1 &= mP_2 + Q_{i_2} \\ P_2 &= mP_3 + Q_{i_3} \\ &\vdots \\ P_n &= mP_{n+1} + Q_{i_{n+1}}. \end{aligned}$$

Durch sukzessives Einsetzen erhalten wir für P: $P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j}$. Da es nur endlich viele der Q_i gibt, müssen wir nur zeigen, dass P_n für n hinreichend groß aus einer endlichen Menge von Elementen kommt. wegen Voraussetzung *(iii)* müssen wir hierzu

nur zeigen, dass $h(P_n)$ für hinreichend großes n unterhalb einer konstanten Schranke liegt, die nicht von P abhängt.

Nun gilt

$$\begin{aligned} h(P_j) &\leq \frac{1}{m^2}(h(mP_j) + C_2) \\ &= \frac{1}{m^2}(h(mP_{j-1} - Q_{i_j}) + C_2) \\ &\leq \frac{1}{m^2}(2h(P_{j-1}) + C_1 + C_2), \end{aligned}$$

wobei $C_1 := \max\{C_1^{-Q_1}..C_1^{-Q_r}\}$. Indem wir diese Ungleichung wiederholt einsetzen, erhalten wir

$$\begin{aligned} h(P_n) &\leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{1}{m^2}\left(1 + \frac{2}{m^2} + \left(\frac{2}{m^2}\right)^2 + .. + \left(\frac{2}{m^2}\right)^{n-1}\right)(C_1 + C_2) \\ &\leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{C_1 + C_2}{m^2 - 2} \\ &\leq 2^{-n}h(P) + (C_1 + C_2)/2, \qquad \text{da } m \geq 2 \end{aligned}$$

und für hinreichend großes n erhalten wir somit $h(P_n) \leq 1 + (C_1 + C_2)/2$. Nach dem obigen ist A nun durch die endliche Menge $\{Q_1, .., Q_r\} \cup \{P \in A | h(P) \leq 1 + (C_1 + C_2)/2\}$ erzeugt. □

Unsere verbleibende Aufgabe ist es nun, eine Höhenfunktion für elliptische Kurven über Zahlkörpern zu finden. Der allgemeine Fall wird Thema der letzten zwei Vorträge sein, für $K = \mathbb{Q}$ definieren wir hier (ohne Beweis) die Höhenfunktion (und diese kann mit der im Anhang zu beobachtenden „Komplexität“ verglichen werden).

Definition 2.2. Sei $E/\mathbb{Q}$ eine elliptische Kurve, und fixiere eine Weierstrass-Gleichung. Die *Höhe* auf $E(\mathbb{Q})$ (bzgl. der Weierstrass-Gl.) ist gegeben durch

$$h_x(P) = \begin{cases} \log\ H(x(P)) & P \neq O \\ 0 & P = O \end{cases},$$

wobei für einen gekürzten Bruch $\frac{a}{b} \in \mathbb{Q}$ $H(\frac{a}{b})$ definiert ist durch $H(\frac{a}{b}) := \max\{|a|, |b|\}$.

Satz 2.3. *h_x ist eine Höhenfunktion im Sinne des Abstiegssatzes.*

Anhang

Auf der nächsten Seite wird für eine elliptische Kurve über $\mathbb{Q}$ ein Erzeuger von $E(\mathbb{Q}) \cong \mathbb{Z}$ gewählt, und die x-Koordinaten seiner Vielfachen (bzgl. einer Weierstrass-Gl.) als gekürzte Brüche ausgegeben. Man sieht, dass die Brüche immer länger werden, und eine kurze Überlegung bestätigt, dass die Länge der Brüche proportional zu $h_x([n]P)$ ist.

Höhe über $\mathbb{Q}$

```
E = EllipticCurve([-2,2]); view(E); view(E.is_smooth());
```

$y^2 = x^3 - 2x + 2$

True

```
P = E.gens()[0]; P #Ein Erzeuger des freien Teils der
Mordell-Weil Gruppe über Q
```

$(1 : 1 : 1)$

```
for i in range(1, 35):
    view ((i*P)[0])
```

1

$-\frac{7}{4}$

$\frac{97}{121}$

$\frac{13729}{144}$

$\frac{1860769}{1525225}$

$-\frac{1252469191}{781873444}$

$\frac{1633982694337}{2713402912081}$

$\frac{35541741012120193}{1490200256084544}$

$\frac{637996549376474433601}{427325931839105897521}$

$-\frac{39781959203403452024292679}{29782647608844772090848100}$

$\frac{434771657461043724338303261 9041}{113244578912302717864471539109 21}$

$\frac{1737000624487718169248087617 4931364513}{163433822399909514012144508740687 1824}$

$\frac{4082120063515262256800776334916256579877 1937}{218651745135665094563299663165425076182438 01}$

$-\frac{2197019191532345266269216072125913861473421718083 91}{219863257828603538181562366648409287259637361421280 4}$

$\frac{1178971777989521474028956327182745523492933720452309574529}{883677121786475933203737218895996517285156366056322773302 5}$

$\frac{1605071747352076982932452087266752090360889306383703121353935784449}{266719836868188058115017866862764512022685802011092862445388392704}$

$\frac{4913429998789103112499465159104554937534521118328205108765281093042660834 57}{202696866551749658907493707831839877572455425426958917468742424142140774881}$

$-\frac{2001785164744249037433875118553309166546824466587194987203704880937469192877863468 87}{312374929675349754808598897292609206403826170677125856576821447054714759564942482244}$

$-\frac{2037638641450750966617766688034395978868826659943605886122449247192716422160417945915325921 59}{1296078423062047357501686782791543517478493845115458437057194234129373271933155160223589945881}$

$\frac{2808184270074837986125202289784756017022537785895342573651561693606167573454755752954364413622853079568 1}{7201368204652717659128816273781742061723435209804478692883685754727229098492422619357590506000736976400}$

$\frac{1117762878000347219840323520933080470379606774630081650345933595330780239891143282230691834328712142135963003615521}{3363949336893088464346435710056194123166756361017093704641057233916334099638991187747123201257393189832305164526 81}$

$-\frac{2518678844013540690957165064822744264104494188601143400710316763380102027214892786075264987890294139704745003287194300455584 7}{8478053712104292338625699980365470076045143895093964517908862568391804101175441450557587798882432562693649489009740581470640 4}$

$-\frac{1751282509219357944719906713092482123973056840215004764869466744773781434850786041551407865953170542493169260957731693911431038463441734 3}{3594826045224269514018408684642329453989145326306285265854795125507412245482041084396642073833536573661720886133196878848783074824608472 1}$

$\frac{9307213940181700763207764504137268675829540063716266987776113873057776874319702356825312860374389433129330105544292381733218733236097705777726 7}{3371160132553751588485952240851481331440726521623959634293714259958165875923052343566671850018866429480576084139453834327480902381770439547339077}$

$\frac{4815846963932594010701902468554113891433143782786313008519152062793290353467754881670755138830700912544723892002439060091903402023185091816258 1}{9802069519849594852989009839962291173640406746104793462951192409564319156531972876252535570622075276019887457595706862588500900005368358250651 31}$

$-\frac{5018178513703858445828436539387173562534048622489695843242850780915399004863551915902425482909485983193330427317196168402699429899214682975393 4364116127022652416412580095805951902410928704193512541269533049457752660152469137560710215996735011581966092944425992489420456865646027872760 6}$

$-\frac{1600040806887922302161515410737048087221538199111195649469239738225549910374332734661720393851450340321803033287732858921506272603096794941 49}{1898581668739850008924235726994903542130680736442837776885564334025227942182284312785570853996201757513873599921201985767455427207003838530 87}$

$\frac{5837053269013611534971106554643924142460350505676732642857927746930558467884938386321591454772405417450802801586047601604261704645544058489675 2804773949798304107189196946492074263942412506550256221208932390648946910659747706650380674764655419109518529925210150960397957989580435660078 4}$

$\frac{3930043303391109870196753092999358328232992741469908576263337622815180463529196848265339260741657813030266722551182980369816912988853794366003 5 48429404018441195559372612521222496583151431884121958390324820093401722807709713049042714888766707222768366773263998001345974593091416841731 21}$

$\frac{1181056773234798946733995099612398763888334536273023410021021259373724033800842023170012620153013471872936140936101384212453397886933224855287 5 42332067387260645213411297294441117324521790522875398680145192560845875831841905217792770841545375657444029724630133332257890747668136733735438}$

$-\frac{2297274738850297048022599624304747644079371890549069235354541116487350349338773699686191354019525166121061062083595322430888014792333639058 3 19235461597464805777891835309492382521101982010069953805227254240609560817862964246698123501079850849967688546510635585227116331756700029015 6}$