Elliptische Kurven

PD Dr. Klaus Haberland

Semester: SS 2009

Vorwort

Dieses Dokument wurde als Skript für die auf der Titelseite genannte Vorlesung erstellt und wird jetzt im Rahmen des Projekts „Vorlesungsskripte der Fakultät für Mathematik und Informatik“ weiter betreut. Das Dokument wurde nach bestem Wissen und Gewissen angefertigt. Dennoch garantiert weder der auf der Titelseite genannte Dozent, die Personen, die an dem Dokument mitgewirkt haben, noch die Mitglieder des Projekts für dessen Fehlerfreiheit. Für etwaige Fehler und dessen Folgen wird von keiner der genannten Personen eine Haftung übernommen. Es steht jeder Person frei, dieses Dokument zu lesen, zu verändern oder auf anderen Medien verfügbar zu machen, solange ein Verweis auf die Internetadresse des Projekts `http://uni-skripte.lug-jena.de/` *enthalten ist.*

Diese Ausgabe trägt die Versionsnummer 2114 und ist vom 9. Mai 2009. Eine neue Ausgabe könnte auf der Webseite des Projekts verfügbar sein.

Jeder ist dazu aufgerufen, Verbesserungen, Erweiterungen und Fehlerkorrekturen für das Skript einzureichen bzw. zu melden oder diese selbst einzupflegen – einfach eine E-Mail an die Mailingliste `<uni-skripte@lug-jena.de>` *senden. Weitere Informationen sind unter der oben genannten Internetadresse verfügbar.*

Hiermit möchten wir allen Personen, die an diesem Skript mitgewirkt haben, vielmals danken:

- *Jens Kubieziel* `<jens@kubieziel.de>` *(2009)*

Inhaltsverzeichnis

Auflistung der Theoreme

Sätze

Definitionen und Festlegungen

0 Einführung

0.1 Die projektive Ebene

Sei K ein beliebiger Körper.

Definition 0.1 (Projektive Ebene)
Die **projektive Ebene** $\mathbb{P}^2(K)$ ist per definitionem $K^3 \setminus \{0,0,0\}/_\sim$, wobei $(x_0, x_1, x_2) \sim (y_0, y_1, y_2) \Leftrightarrow \exists \lambda \in K^*$ mit $y_j = \lambda x_j$. Man schreibt $(x_0 \colon x_1 \colon x_2)$.

Bemerkung 0.1
Analog $\mathbb{P}^n(K)$ für $n \geq 1$.

Beispiel 0.1
Man nennt $\mathbb{P}^1(K)$ die projektive Gerade und ist $\mathbb{P}^1(K) = \{(1 \colon \alpha) \colon \alpha \in K\} \cup \{(0 \colon 1)\}$. Das ist also die affine Ebene vereinigt mit einem unendlich fernen Punkt.

Es ist $\mathbb{P}^1(\mathbb{R}) = \mathbb{R}$ plus ∞, also die S^1-Kreislinie. Für $\mathbb{P}^1(\mathbb{C})$ ergibt sich S^2, die auch als Riemannsche Zahlensphäre bezeichnet wird.

Weiter haben wir $\mathbb{P}^1(\mathbb{F}_2) = \{(0 \colon 1), (1 \colon 0), (1 \colon 1)\}$.

Bemerkung 0.2 (Affine Überdeckung von $\mathbb{P}^n(K)$)
Sei $U_i = \{(x_0 \colon x_1 \colon \ldots \colon x_n) \colon x_i \neq 0\}, \varphi_i \colon U_i \to A^n(K)$ mit $(x_0 \colon x_1 \colon \ldots \colon x_n) \mapsto (x_0/x_i, x_1/x_i, \ldots, \hat{x_i/x_i}, \ldots, x_n/x_i)$. Die inverse Abbildung dazu ist, $\psi \colon A^n(K) \to U_i$ mit $(y_1, \ldots, y_n) \mapsto (y_1 \colon \ldots \colon y_i \colon 1 \colon y_{i+1} \colon \ldots \colon y_n)$. Insbesondere ist $\mathbb{P}^2(K) = U_0 \dot\cup \mathbb{P}^1(K)$.

Für $K = \mathbb{R}$ haben wir, $S^2 \subset \mathbb{R}^3 \setminus (0,0,0) \to \mathbb{P}^2(\mathbb{R})$. Man bezeichnet $S^2 \to \mathbb{P}^2(\mathbb{R})$ als zweiblättrige Überlagerung.

$\mathrm{GL}(n+1, K)$ operiert auf $\mathbb{P}^n(K)$ vermöge

$$g(x_0 \colon x_1 \colon \ldots \colon x_n) = (g_0 x \colon g_1 x \colon \ldots \colon g_n x)$$

Beispiel 0.2
Es operiert $\mathrm{GL}(2, \mathbb{F}_2)$ auf $\mathbb{P}^1(\mathbb{F}_2) = \{0,1,\infty\}$. Die Aktion ist transitiv. Also haben wir einen injektiven Homomorphismus $\mathrm{GL}(2, \mathbb{F}_2) \to S_3$. Denn $\begin{pmatrix} a & b \\ c & d \end{pmatrix} (0 \colon 1) = (0 \colon 1) \Leftrightarrow b = 0, d = 1$ und $\begin{pmatrix} a & b \\ c & d \end{pmatrix} (1 \colon 0) = (1 \colon 0) \Leftrightarrow a = 1, c = 0$. Damit folgt, dass $\mathrm{SL}(2, \mathbb{F}_2)$ isomorph zu S_3 ist.

0.2 Ebene projektive Kurven

Sei $F \in K[X_0, X_1, X_2]$ homogen vom Grad d.

Definition 0.2 (ebene algebraische Kurve)
Eine **ebene algebraische Kurve** ist der Nullstellenort eines homogenen Polynoms $F \in K[X_0, X_1, X_2]$ in $\mathbb{P}^2(K)$.

Fakt
Diese Definition ist korrekt, da homogen vorausgesetzt wird.

Beweis:
$F(\lambda x_0, \lambda x_1, \lambda x_2) = \lambda^d F(x_0, x_1, x_2)$ ∎

Bemerkung 0.3
Sei $C_F(K) = \{(x_0 \colon x_1 \colon x_2) \in \mathbb{P}^2(K) \colon F(x_0, x_1, x_2) = 0\}$ und L/K eine Körpererweiterung. Dann gilt $C_F(K) \subset C_F(K)$.

Beispiel 0.3

1. Die Fermat-Kurven: Sei $d \geq 2, F = x^d + y^d - z^d \in \mathbb{Q}[X, Y, Z]$. Was sind die unendlich fernen Punkte? $z = 0$! Also $x^d + y^d = 1 \Rightarrow y = (-1)^{1/d} x$ und somit $(1 \colon \xi \colon 0), \xi^d = -1$. Es hat $C_d(\mathbb{R})$ einen unendlich fernen Punkt für gerade d und keinen für gerades d.

   Sei nun d ungerade. Dann ist $C_d(\mathbb{Q}) = \{(0 \colon 1 \colon 1), (1 \colon 0 \colon 1), (1 \colon -1 \colon 0)\}$. Für $C_2(\mathbb{Q})$ kennt man alle rationalen Punkte. Weiter hat $C_4(\mathbb{Q})$ nur die trivialen rationalen Punkte (nach Fermat).

2. Hyperelliptische Kurven: $y^2 = f(x)$ mit $f \in K[X]$ oder homogen, $y^2 z^{d-2} = f(x/z) z^d$ mit d gleich dem Grad von f. Ist der Grad von f größer oder gleich 5 und $y^2 - f(x) \in \overline{\mathbb{Q}}[X, Y]$ irreduzibel, so ist $C_F(\mathbb{Q})$ endlich (nach Faltings).

Definition 0.3 (irreduzibel)
Die projektive ebene Kurve C_F mit $F \in K[X, Y, Z]$ homogen heißt **irreduzibel**, wenn F irreduzibel in $\overline{K}[X, Y, Z]$ ist.

Definition 0.4 (glatt, regulär)
Der Punkt $P \in C_F(\overline{K})$ heißt **glatt** oder **regulär**, wenn der Gradient von F im Punkt p ungleich 0 ist. Also hat die Kurve in dem Punkt eine Tangente.

Man bezeichnet C_F als **glatt** oder **singularitätenfrei**, wenn alle $P \in C_F(\overline{K})$ glatt sind.

Beispiel 0.4

1. $(xyz = 0) = C$, $C = C_0 \cup C_1 \cup C_2, C_0 = (x = 0), C_1 = (y = 0), C_2 = (z = 0)$. Es ist C die Vereinigung dreier projektiver Geraden in $\mathbb{P}^2(K)$. Singulär sind genau die Schnittpunkte:$(1 \colon 0 \colon 0), (0 \colon 1 \colon 0), (0 \colon 0 \colon 1)$.

2. Die Fermat-Kurven: $\operatorname{grad}(x^d + y^d + z^d) = (dx^{d-1}, dy^{d-1}, dz^{d-1})$. Also sind die Kurven glatt.

3. Hyperelliptische Kurven: $y^2z^{d-2} = f(x/z)z^d = a_0z^d + a_1z^{d-1}x \cdots + a_dx^d$. Für den Gradient ergibt sich: $(z^{d-1}f'(x/z), -2yz^{d-2}, -z^{d-2}xf'(x/z) + dz^{d-1}f(x/z))$. Unendlich ferne Punkte: $z = 0, d > 2 \Rightarrow x = 0$, nur $(0\colon 1\colon 0)$. In $(0\colon 1\colon 0)$ ist der Gradient (0,0,0), also ist der Punkt singulär.

1 Quadriken

1.1 Allgemeines

Definition 1.1 (Quadrik)
Eine **Quadrik** ist eine ebene projektive Kurve definiert durch quadratische Form:

$$C = C_F F = aX^2 + bXY + cXZ + dY^2 + eYZ + fZ^2$$

Bemerkung 1.1
Für $\lambda \in K^*$ ist $C_{\lambda F} = C_F$. Wir setzen voraus, dass die Charakteristik des Körpers nicht 2 ist.

$$M_F :- \begin{pmatrix} a & b/2 & c/2 \\ b/2 & d & d/2 \\ c/2 & e/2 & f \end{pmatrix}$$

$$F = (X, Y, Z) M_F \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

Definition 1.2 (linear isomorph)
Zwei Quadriken C_F, C_G heißen **linear isomorph**, wenn es ein $g \in \mathrm{GL}(3, K)$ mit $G = F \circ g \Leftrightarrow M_G = g^T M_F g$ gibt.

Definition 1.3 (Rang)
Der **Rang** von F ist als der Rang von M_F definiert.

Fakt
Jede quadratische Form ist linear äquivalent zu einer Diagonalform.

Beweis:
Ist $v^T M v = 0$ für alle $v \in K^3$, so ist $M = 0$. Das Einsetzen von e_1, e_2, e_3 zeigt $a = d = f = 0$ und $e_1 + e_2, e_2 + e_3, e_3 + e_1$ zeigt $b = c = e = 0$. Wir wählen also $v \neq 0$ mit $v^T M v :- \alpha \neq 0$ und bilden $g \in \mathrm{GL}(3, K)$ mit v als erster Spalte. Dann hat $g^T M g$ links oben den Eintrag α. Die zugehörige Form ist $G = \alpha X^2 + \beta XY + \gamma XZ + H(Y, Z) = \alpha(X + 1/2 \beta/\alpha Y + 1/2 \gamma/\alpha Z)^2 + H_1(Y, Z)$. Also ist F linear äquivalent zu $F_1 = \alpha X^2 + H_1(Y, Z)$. Der Rest ergibt sich durch Induktion. ∎

Bemerkung 1.2
Der Rang von $aX^2 + bY^2 + cZ^2$ ist die Anzahl der Koeffizienten, die ungleich Null sind.

Fakt
Die Kurve C_F ist genau dann glatt, wenn der Rang von F gleich 3 ist.

Beweis:
Die Glattheit erhält sich unter linearen Substitutionen. Also sei o. B. d. A. $F = aX^2 + bY^2 + cZ^2$ und für den Gradient ergibt sich $2(aX, bY, cZ)$. Ist der Rank 3, so ist $abc \neq 0$ und somit ist C_F glatt.

Sei nun der Rang kleiner als 3. Für $c = 0$ ist $F = aX^2 + b^2$ und $(0\colon 0\colon 1)$ ist singulärer Punkt auf C_F. ∎

Fakt
Sei C_F glatt und $C_F(K) \neq \emptyset$. Dann existiert eine Bijektion zwischen $C_F(K)$ und der projektiven Geraden $\mathbb{P}^1(K)$.

Beweis:
Seo $P_0 \in C_F(K) \subset \mathbb{P}^2(K)$ und $H \subset \mathbb{P}^2(K)$ eine projektive Gerade, die P_0 nicht enthält. Sei $\varphi\colon H \to C_F(K)$ mit $P \mapsto$ Schnittpunkt der projektiven Geraden L durch P und P_0 mit $C_F(K)$. Es schneidet L die Kurve $C_F(K)$ in P_0 und deshalb noch in einem weiteren Punkt. Dieser liegt auch in $C_F(K)$.

Die inverse Abbildung ist $\psi\colon C_F(K) \to H$, die P auf den Schnitt der Geraden durch P und P_0 mit H abbildet. Für $P = P_0$ nehme man die Tangente an $C_F(K)$. ∎

1.2 Die Quadriken über $\mathbb{R}$ und $\mathbb{C}$

1. Über $\mathbb{C}$ ist jede Quadrik linear äquivalent zu

   $$X^2 + Y^2 + Z^2$$

   (isomorph zu $\mathbb{P}^2(\mathbb{C})$, gewöhnliche Quadrik in $\mathbb{P}^2(\mathbb{C})$.) oder

   $$X^2 + Y^2$$

   (zwei transversale projektive Gerade in $\mathbb{P}^2(\mathbb{C})$) oder

   $$X^2$$

   (doppelte projektive Gerade) oder

   $$0$$

   $\mathbb{P}^2(\mathbb{C})$

2. über $\mathbb{R}$:

$$X^2 + Y^2 + Z^2 \qquad\qquad X^2 + Y^2 - Z^2$$

Das erstgenannte ist die leere Menge und das zweite ist eine gewöhnliche Quadrik in $\mathbb{P}^2(\mathbb{R})$

$$X^2 + Y^2 \qquad\qquad X^2 - Y^2$$

Erstes ist $(0\colon 0\colon 1)$ und das Zweite sind zwei transversale projektive Geraden

$$X^2$$

zweifache projektive Gerade

$$0$$

$\mathbb{P}^2(\mathbb{R})$

1.3 Quadriken über endlichen Körpern

Wie schon oben setzen wir wieder voraus, dass die Charakteristik des Körpers ungleich 2 ist. Weiter sei $K = \mathbb{F}_q$ mit $q = p^f$ für p größer als 2. Wir behandeln nur glatte Quadriken. Jede solche Quadrik lässt sich bis auf lineare Äquivalenz durch

$$X^2 + Y^2 + Z^2$$

oder

$$X^2 + Y^2 + \lambda Z^2$$

beschreiben. Dabei ist λ ein fixiertes Nichtquadrat in $\mathbb{F}_q^*$.

Fakt
$C_F(\mathbb{F}_q)$ ist stets nichtleer für C_F glatt.

Beweis:
Der Beweis erfolgt durch Zählen. Dazu wählen wir $z_0 \in K^*$ und setzen $\alpha = -z_0^2$ im ersten Fall und $\alpha = -\lambda z_0^2$ im zweiten Fall. Dann produzieren die Polynome X^2 und $\alpha - Y^2$ jeweils $\frac{q+1}{2}$ verschiedene Werte. Also muss es $x_0, y_0 \in K$ mit $x_0^2 = \alpha - y_0^2$ geben. ∎

Folgerung
$\operatorname{card} C_F(\mathbb{F}_q) = q + 1$

Beispiel 1.1
Wir betrachten die Kreislinie $x^2 + y^2 = 1$ in $\mathbb{F}_q^2$. Das sind gerade die Punkte auf $\{x^2 + y^2 - z^2 = 0\} \subset \mathbb{P}^2(\mathbb{F}_q)$, weche im Endlichen liegen. Unendlich ferne Punkte sind die mit $z = 0$, also $x^2 + ^2 = 0 \Leftrightarrow (\frac{x}{y})^2 = -1$. Ist also -1 kein Quadrat in $\mathbb{F}_q^*$, so liegen alle $q + 1$ Punkte im Endlichen. Somit hat die Kreislinie $q + 1$ Punkte. Ist dagegen -1 ein Quadrat in $\mathbb{F}_q^*$, liegen auf der Kreislinie $q - 1$ Punkte. Für $q = p \in \mathbb{P}$ gilt, dass -1 genau dann ein Quadrat, wenn $p \equiv 1 \pmod 4$.

Beispiel 1.2
Für $p = 7$ hat $x^2 + y^2 = 1$ insgesamt acht Lösungen.

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1
$1 - x^2$	1	0	4	6	6	4	0

1.4 Quadriken über $\mathbb{Q}_p$

Details zu p-adischen Zahlen kann man in [8] nachlesen. Wir betrachten nur glatte Quadriken:

$$C = \{ax^2 + by^2 + cz^2 = 0\} \subset \mathbb{P}^2(\mathbb{Q}_p)$$

Bis auf lineare Äquivalenz und Skalare nur zwei Typen:

1. $a, b, c \in \mathbb{Z}_p^*$
2. $a, b \in \mathbb{Z}_p^*, c \in p\mathbb{Z}_p^*$

Fakt

1. Im ersten Fall ist $C(\mathbb{Q}_p)$ stets nichtleer.
2. Im zweiten Fall ist $C(\mathbb{Q}_p)$ genau dann nichtleer, wenn gilt $-ab$ ist Quadrat modulo p oder genau dann, wenn $\left(\frac{-ab}{p}\right) = 1$.

Beweis:

1. Nach Abschnitt 1.3 hat die Kongruenz $ax^2 + by^2 + cz^2 \equiv 0 \pmod p$ nichttriviale Lösung, d. h. es gibt ein $(x_0, y_0, z_0) \in \mathbb{Z}_p^3$, nicht alle drei durch p teilaren mit $ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod p$. Sei beispielsweise $x_0 \equiv 0 \pmod p$. Setze $f() = at^2 + by_0^2 + cz_0^2 \in \mathbb{Z}_p[t]$. Dann ist $|f(x_0)|_p < 1, f'(x_0) = 2ax_0, |f'(x_0)|_p = 1$. Nach Hensels Lemma existiert ein $x \in \mathbb{Z}_p$ mit $x \equiv x_0 \pmod p$ mit $f(x) = 0 \Rightarrow$ nichttriviale Lösung.

2. Angenommen die Kurve $C(\mathbb{Q}_p)$ hat einen rationalen Punkt. Also existieren $x, y, z \in \mathbb{Z}_p, (x, y, z) \neq (0,0,0)$ mti $ax^2 + by^2 + cz^2 = 0$. Seien alle o. B. d. A. durch p teilbar. Ist $x \equiv 0 \pmod p$, so auch y. Mithin $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p^2} \Rightarrow cz^2 \equiv 0 \pmod{p^2} \Rightarrow z \equiv 0 \pmod p$ ↯ Also sind x, y, z Einheiten. Weiter $ax^2 + by^2 \equiv 0 \pmod p$ wegen $p \mid c$. Dann ist $abx^2 \equiv -(by)^2 \pmod p$ und $-ab \equiv (by/x)^2 \pmod p$. Also folgt, dass $-ab$ Quadrat modulo p ist.

   Hensels Lemma im Anhang erklaeren

   Sei nun $-ab$. Dann ist $-ab$ nach Hensels Lemmaein Quadrat in $\mathbb{Z}_p^*$. Somit $-ab = t^2$ für $t \in \mathbb{Z}_p^*$. Also ist $at^2 + ba^2 = 0$ nichttriviale Lösung $(t, a, 0)$. ∎

Vorlesungen vom 2009-04-22/23

2 Elliptische Kurven über $\mathbb{C}$

2.1 Gitter und Tori

Definition 2.1 (Gitter)
Man bezeichnet $L \subset \mathbb{C}$ als **Gitter**, wenn gilt: $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ mti $\omega_1, \omega_2 \in \mathbb{C}$ und $\mathbb{R}$-linear unabhängig. Man bezeichnet ω als **Periode**n des Gitters.

Definition 2.2
Sei f eine meromorphe Funkton auf $\mathbb{C}$, $L \subset \mathbb{C}$ ein Gitter. Die Funktion f heißt ***L*-elliptisch**, wenn gilt $f(z+\omega) = f(z)$ für alle $z \in \mathbb{C}$ und $\omega \in L$.

Verweis auf Literatur einfügen

Bemerkung 2.1

1. Die f sind gerade die meromorphen Funktionen auf $X = \mathbb{C}/L$.
2. Die Menge $\mathbb{C}(X)$ aller L-elliptischen Funktionen ist ein Körper. Mit f ist auch f' eine L-elliptische Funktion.

Beispiel 2.1
Meromorphe Funktion auf $\mathbb{P}^1\mathbb{C}$. Das sind die meromorphen Funktionen auf $\mathbb{C}$, welche in ∞ höchstens einen Pol haben. Wir zerlegen $\mathbb{P}^1\mathbb{C} = U_0 \cup U_1$ und nehmen $f \in \mathbb{C}(\mathbb{P}^1(\mathbb{C}))$. Es ist $f|U_0 = \varphi(u)$ meromorph auf $\mathbb{C}$, $f|U_1 = \psi(v)$ meromorph auf $\mathbb{C}$ mit $v = z_0/z_1$. Es gilt $u \cdot v = 1$. Mithin $v^m\psi(v)$ holomorph in $0 \Rightarrow v^{-m}\varphi(u)$ ist normbeschränkt um ∞, meromorph $\Rightarrow v^{-m}\varphi(u) = \frac{1}{P(u)}$ mit P Polynom. Also ist f rational. Somit $\mathbb{C}(\mathbb{P}^1(\mathbb{C})) = \mathbb{C}(T)$ mit T Unbestimmte.

Definition 2.3 (Ordnung)
Sei $z_0 \in \mathbb{C}$ und f meromorph um z_0. Die **Ordnung** von f ist definiert als $(z - z_0)^m g(z)$. Dabei ist g holomorph in z_0 und $g(z_0) \neq 0$.

Bemerkung 2.2

1. $\operatorname{ord}_{z_0}(fg) = \operatorname{ord}_{z_0}(f) + \operatorname{ord}_{z_0}(g)$
2. $\operatorname{ord}_{z_0}(f+g) \geq \min(\operatorname{ord}_{z_0}(f), \operatorname{ord}_{z_0}(g))$
3. $\operatorname{ord}_{z_0}(f') = \operatorname{ord}_{z_0} f - 1$
4. Die Ordnung der Nullfunktion ist plus Unendlich.
5. Falls f eine L-elliptische Funktion ist, so gilt: $\operatorname{ord}_{z_0} f = \operatorname{ord}_{z_0+\omega} f$ für alle $\omega \in L$. Also ist $\operatorname{ord}_p f$ wohldefiniert für $p \in \mathbb{C}/L = X$.

Definition 2.4 (Divisorengruppe)
Sei $X = \mathbb{C}/L$. Dann ist die **Divisorengruppe** von X die freie abelsche Gruppe über den Punkten von X. Also ist ein **Divisor** formal die $\mathbb{Z}$-Linearkombination endlich vieler Punkte aus X. Wir schreiben $\mathrm{Div}(X)$ und $D = \sum m_p P = \sum m_p [P]$ mit $m_p \in \mathbb{Z}$.

Definition 2.5 (Hauptdivisor)
Jeder L-elliptischen Funktion $f \in \mathbb{C}(X)^*$ kann man einen Divisor $(f) = \div(f)$ vermöge $(f) = \sum_{P \in X} \mathrm{ord}_p(f) \cdot P$ zuordnen. Diese Divisoren heißen **Hauptdivisoren**.

Die Abbildung

$$\div \colon \mathbb{C}(X)^* \to \mathrm{Div}(X)$$

ist ein Homomorphismus. Der Kern ist $\mathbb{C}^*$.

Beweis:
$\div(f)$ ist tatsächlich ein Divisor: Ist $\mathrm{ord}_p(f) \neq 0$, so hat f auf einer offenen Umgebung weder Pole noch Nullstellen. Wegen der Kompaktheit von X ist also auch $\mathrm{ord}_p(f) \neq 0$ nur für endlich viele $P \in X$. ∎

Definition 2.6 (Picard-Gruppe)
$\mathrm{Pic}(X) = \mathrm{Div}(X)/\operatorname{Im} \mathbb{C}(X)^*$ heißt **Picard-Gruppe** von X. Weiter heißt $\deg \colon \mathrm{Div}(X) \to \mathbb{Z}$ mit $\sum m_p P \mapsto \sum m_p$ heißt der **Grad** von D. Die Abbildung ist ein Homomorphismus.

Beispiel 2.2
$X = \mathbb{P}^1\mathbb{C}, \mathbb{C}(X) = \mathbb{C}(T), \ker \div = \mathbb{C}^*$. Wir zeigen: Das Bild ist $\mathrm{Div}^0(X) = \{D \in \mathrm{Div}(X) \colon \deg D = 0\}$. Sei dazu $D = \sum m_j z_j + m_\infty \infty$ und $\sum m_j + m_\infty = 0$. Es ist $f := \prod_{j=1}^N (z - z_j)^{m_j} \in \mathbb{C}(X)$. Der Divisor von f ist $(f) = \sum_{j=1}^N m_j z_j + m\infty$. Das m wird so berechnet: Ersetze z durch $1/u$: $f(1/u) = \prod (1/u - z_j)^{m_j} = u^{-\sum m_j} \prod (1 - u z_j)^{m_j} = u^{m_\infty} \prod) 1 - u z_j)^{m_j}$. Bei $u = 0$ ist die Ordnung also m_∞ und $m = m_\infty$. Also ist $\mathrm{Pic}(\mathbb{P}^1\mathbb{C}) = \mathbb{Z}$.

Bemerkung 2.3
Zur Einheit der Mathematik: Sei K ein algebraischer Zahlkörper, $\mathrm{Div}(K)$ die freie abelsche Gruppe über den maximalen Idealen vom Ring der ganzen Zahlen O_K. Dann sind die Divisoren die gebrochenen Ideale in K.

$$K^* \to \mathrm{Div}(K) \colon \alpha \mapsto \sum_{g \subset O_K} \mathrm{ord}_g(\alpha) g$$

Der Kern sind die Einheiten $E_K = O_K^*$. Man hat eine exakte Sequenz: $O \to E_K \to K^* \to \mathrm{Div}(K) \to \mathrm{Cl}_K \to 0$.

Fakt
Sei $X = \mathbb{C}/L$ und $f \in \mathbb{C}(X)^*$ eine meromorphe Funktion. Dann gilt:

1. $\deg \div(f) = 0$
2. $\sum_{P \in X} \mathrm{Res}_P(f) = 0$

3. $\sum_{P\in X} \operatorname{ord}_p(f)[P] = 0$ in $X = \mathbb{C}/L$

Beweis:

1. Wende (ii) auf die Funktion f'/f an. Dann ist $\operatorname{Res}_P f'/f = \operatorname{ord}_p(f)$: $f(z) = z^m g(z)$ mit g holomorph und $g(0) \neq 0$. Damit haben wir $f'/f = m/z + \frac{g'(z)}{g(z)}$.

2. Sei $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, Q_a = \{a + t\omega_1 + u\omega_2 \colon 0 \leq t, u \leq 1\}$. Man bezeichnet Q_0 als **Periodenparallelogramm**. Das a lässt sich so wählen, dass auf dem Rand von Q_a keine Pole oder Nullstellen von f liegen. $\int_{\partial Q_a} f(z)\,dz = 2\pi i \sum_{\partial \mathring{Q}_a} \operatorname{Res}_P(f) = 2\pi i \sum_{P\in X} \operatorname{Res}_P(f)$ Das Integral links ist aber 0.

3. Nun nehmen wir $h(z) = \frac{zf'(z)}{f(z)}$. Achtung: Die Abbildung h ist *nicht* L-elliptisch, wohl aber meromorph auf $\mathbb{C}$. Wir wählen das a so, dass $0 \notin Q_a$. Jetzt integrieren wir: $\int_{\partial Q_a} h(z)\,dz = 2\pi i \sum_{P\in \mathring{Q}_a} \operatorname{Res}_P(h) = 2\pi i \sum_{P\in \mathring{Q}_a} P \operatorname{ord}_p(f)$. Sei $I_2 = \int_{a+\omega_1}^{a+\omega_1+\omega_2} h(z)\,dz - \int_a^{a+\omega_2} h(z)\,dz$. Es ist $h(z+\omega_2) = (z+\omega_2)f'/f(z) = h(z) + \omega_2 f'/f(z)$. Nun substituiere man im ersten Integral $z = u + \omega_1$. Dann läuft u von a nach ω_1. Also folgt: $I_2 = \omega_2 \int_a^{a+\omega_1} f'/f(z)\,dz = \omega_2(\log f(a+\omega_1) - \log f(a))$. Das Ergebnis ist $2\pi i$ multipliziert mit einer ganzen Zahl. Wir schreiben hierfür $2\pi i k_2 \omega_2$ und analog $I_1 = 2\pi i k_1 \omega_1$ mit $k_1 \in \mathbb{Z}$. Somit $\sum_{P\in \mathring{Q}_a} \operatorname{ord}_p(f) P = k_1\omega_1 + k_2\omega_2 \in L$. Durch Übergang zum Torus folgt $\sum_{P\in X} \operatorname{ord}_p(f) P = 0$ in $\mathbb{C}/L = X$. ∎

Bemerkung 2.4
Wir haben eine Sequenz $0 \to \mathbb{C}^* \to \mathbb{C}(X)^* \to \operatorname{Div}^0(X) \xrightarrow{\text{sum}} X \to 0$. Dabei ist $\operatorname{sum}(\sum m_p[P]) = \sum m_p P$ in X. Wir kennen fast die Exaktheit dieser Sequenz. Es fehlt nur noch: $\operatorname{sum}(D) = 0 \Rightarrow D = (f)$ für ein $f \in \mathbb{C}(X)^*$. Dies ist Inhalt des Satzes von Abel-Jacobi.

Bemerkung 2.5
Wir wissen noch gar nicht, ob es überhaupt nichtkonstante elliptische Funktionen gibt. Die Idee ist: f meromorph auf $\mathbb{C}$, $g(z) = \sum_{\omega\in L} f(z+\omega)$. Dann ist g eine L-periodische Funktion.

Definition 2.7 (Weierstrasssche $\wp$-Funktion)
Sei L ein Gitter, $z \in \mathbb{C}$. Dann ist $\wp(z, L) :- 1/z^2 \sum_{\substack{\omega\in L \\ \omega\neq 0}} (\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$.

Literaturverzeichnis

[1] Anthony W. Knapp. Elliptic curves. Princeton, NJ. Princeton University Press, 1992.

[2] Dale Husemöller. Elliptic curves. Graduate texts in mathematics, v. 111. New York. Springer, 2003.

[3] Neal Koblitz. Introduction to elliptic curves and modular forms. Graduate texts in mathematics, 97. New York. Springer-Verlag, 1984.

[4] Joseph H. Silverman. The arithmetic of elliptic curves. Graduate texts in mathematics, 106. New York. Springer-Verlag 1986.

[5] Joseph H. Silverman. Advanced topics in the arithmetic of elliptic curves. Graduate texts in mathematics, 151. Springer-Verlag, 1994.

[6] Joseph H. Silverman und John Torrence Tate. Rational points on elliptic curves. Undergraduate texts in mathematics. New York. Springer-Verlag, 1992.

[7] James S. Milne. Elliptic curves. http://www.jmilne.org/math/.

[8] Jean-Pierre Serre. A course in arithmetic. New York. Springer-Verlag, 1973.

Index