Diophantische Geometrie

Wolfgang M. Ruppert

Wintersemester 1995/96

19. März 1999 [1]

[1] Im Wintersemester 1995/96 am Mathematischen Institut der Universität Erlangen abgehaltene Vorlesung

Inhaltsverzeichnis

KAPITEL 1

Einführung

Gegeben seien Polynome $f_1, \ldots, f_r \in \mathbf{Z}[x_1, \ldots, x_n]$. Ist R ein kommutativer Ring (mit Eins), so kann man die f_i's als Elemente von $R[x_1, \ldots, x_n]$ betrachten und definieren

$$\begin{aligned} X(R) &= \{P \in R^n : f_1(P) = \cdots = f_r(P) = 0\} = \\ &= \{(a_1, \ldots, a_n) \in R^n : f_1(a_1, \ldots, a_n) = \cdots = f_r(a_1, \ldots, a_n) = 0\}. \end{aligned}$$

In der Zahlentheorie ist ein Grundproblem die Bestimmung von $X(\mathbf{Z})$ bzw. $X(\mathbf{Q})$, d.h. das Lösen des diophantischen Gleichungssystems $f_1 = \cdots = f_r = 0$ in ganzen bzw. rationalen Zahlen.
$X(\mathbf{C})$ ist eine algebraische Varietät über $\mathbf{C}$ und wird in der algebraischen Geometrie studiert. Es gilt:

$$X(\mathbf{Z}) \subseteq X(\mathbf{Q}) \subseteq X(\mathbf{R}) \subseteq X(\mathbf{C}).$$

In der diophantischen Geometrie werden qualitative Aussagen über $X(\mathbf{Z})$ und $X(\mathbf{Q})$ in Abhängigkeit von der Geometrie von $X(\mathbf{C})$ gemacht.

Beispiel: $f = 2x + 3y + 5$. Die Bestimmung von $X(\mathbf{Q})$ ist trivial, denn man kann die Gleichung $f = 0$ nach y auflösen:

$$X(\mathbf{Q}) = \{(x, \frac{-2x-5}{3}) : x \in \mathbf{Q}\}.$$

Wann ist $(x, \frac{-2x-5}{3})$ in $X(\mathbf{Z})$? Genau dann, wenn $x \in \mathbf{Z}$ und $3 | 2x + 5$, was äquivalent zu $x \equiv 2 \bmod 3$ ist. Man kann also schreiben $x = 3n + 2$ und damit $y = \frac{-2x-5}{3} = \frac{-6n-9}{3} = -2n - 3$, d.h.

$$X(\mathbf{Z}) = \{(3n + 2, -2n - 3) : n \in \mathbf{Z}\}.$$

Geometrisch beschreibt $f = 0$ eine Gerade in der Ebene.

Beispiel: $f = 2x^2 + 3y^2 + 5$. Man sieht sofort, daß $f = 0$ keine reellen, also erst recht keine rationalen Lösungen besitzt.

Beispiel: Sei $f = 2x^2 + 3y^2 - 1$ und $X = \{f = 0\}$. Offensichtlich ist $X(\mathbf{R}) \neq \emptyset$; $X(\mathbf{R})$ ist eine Ellipse im $\mathbf{R}^2$. Man sieht weiter:

$$X(\mathbf{R}) \subseteq \{(x, y) \in \mathbf{R}^2 : |x| \leq \frac{1}{\sqrt{2}}, |y| \leq \frac{1}{\sqrt{3}}\},$$

woraus man sofort $X(\mathbf{Z}) = \emptyset$ sieht. Wir wollen nun $X(\mathbf{Q})$ bestimmen. Wir setzen an $x = \frac{X}{Z}, y = \frac{Y}{Z}$ und erhalten die Gleichung $g = 2X^2 + 3Y^2 - Z^2 = 0$. Hier müssen wir die ganzzahligen Lösungen bestimmen. Wir können $ggT(X, Y, Z) = 1$ annehmen, da die Gleichung homogen ist. Betrachtung modulo 3 liefert $X \equiv Z \equiv 0 \bmod 3$, d.h. $X = 3X_1, Z = 3Z_1$. Setzt man dies in $g = 0$ ein, so erhält man sofort $Y \equiv 0 \bmod 3$, also $Y = 3Y_1$, ein Widerspruch zu $ggT(X, Y, Z) = 1$. Also erhalten wir $X(\mathbf{Q}) = \emptyset$.

Wir wollen das Phänomen etwas abstrakter formulieren: Ist $X = \{f_1 = \cdots = f_r = 0\}$ mit ganzzahligen Polynomen $f_1, \ldots, f_r$ und $N \geq 2$ ein natürliche Zahl, so erhält man durch Reduktion modulo N eine Abbildung $X(\mathbf{Z}) \to X(\mathbf{Z}/N\mathbf{Z})$. Durch geschickte Wahl von N kann man manchmal Aussagen über $X(\mathbf{Z})$ erhalten. $X(\mathbf{Z}/N\mathbf{Z})$ ist eine endliche Menge. Ist $X(\mathbf{Z}/N\mathbf{Z}) = \emptyset$, so auch $X(\mathbf{Z}) = \emptyset$. Doch auch in anderen Fällen kann man manchmal Rückschlüsse ziehen aus obiger Abbildung. (Siehe voriges Beispiel.)

Beispiel: Sei $f = 2x^2 + 3y^2 - 5$ und $X = \{f = 0\}$. Man sieht schnell $X(\mathbf{Z}) = \{(\pm 1, \pm 1)\}$. Um die rationalen Punkte zu berechnen, legen wir eine Gerade mit Steigung t durch den bereits bekannten Punkt $(1, 1)$ (Geradengleichung $\frac{y-1}{x-1} = t$) und schneiden mit der Kurve $f = 0$, indem wir $y = 1 + t(x - 1)$

in $f=0$ einsetzen: $2x^2+3(1+t(x-1))^2-5=0$. Dies ist eine quadratische Gleichung in x, wobei wir eine Lösung $x=1$ bereits kennen, also sollte sich die zweite auch leicht bestimmen lassen:

$$2x^2+3(1+t(x-1))^2-5=(x-1)[(3t^2+2)x-(3t^2-6t-2)].$$

Die zwei Schnittpunkte der Geraden mit $f=0$ sind also $x=1, y=1$ und

$$x=\frac{3t^2-6t-2}{3t^2+2}, \quad y=\frac{-3t^2-4t+2}{3t^2+2}.$$

Damit hat man alle rationalen Lösungen parametrisiert gegeben:

$$X(\mathbf{Q})=\{(\frac{3t^2-6t-2}{3t^2+2},\frac{-3t^2-4t+2}{3t^2+2}):t\in\mathbf{Q}\}\cup\{(1,1),(1,-1)\}.$$

Bemerkung: Hat man eine quadratische Gleichung $f(x,y)=0$ und einen Punkt $P=(x_0,y_0)\in\mathbf{Q}^2$ mit $f(P)=0$, so kann man obiges Verfahren immer anwenden.

Beispiel: $f=2x^2-3y^2+1$. Man sieht sofort $(1,1)\in X(\mathbf{Z})$. Wie eben findet man eine Parametrisierung

$$x=\frac{3t^2-6t+2}{3t^2-2}, \quad y=\frac{-3t^2+4t-2}{3t^2-2},$$

womit man direkt $X(\mathbf{Q})$ angeben kann. $X(\mathbf{R})$ ist eine Hyperbel im $\mathbf{R}^2$, woraus man noch keine Abschätzung für die ganzzahligen Lösungen erhält. Im Bereich $|x|\leq 10^6$ erhält man durch Computersuche folgende ganzzahlige Lösungen:

$$(\pm x,\pm y)=(1,1),(11,9),(109,89),(1079,881),(10681,8721),(105731,86329).$$

Wir formen die Gleichung etwas um: $(2x)^2-6y^2=-2$. In $\mathbf{Z}[\sqrt{6}]$ suchen wir Elemente der Norm -2. Nun ist der Ring Hauptidealring mit $5+2\sqrt{6}$ Grundeinheit. Die gesuchten Elemente sind $(2+\sqrt{6})(5+2\sqrt{6})^n$ mit $n\geq 0$. D.h.

$$2x_n+y_n\sqrt{6}=(2+\sqrt{6})(5+2\sqrt{6})^n.$$

Anders ausgedrückt:

$$x_n=\frac{1}{4}[(2+\sqrt{6})(5+2\sqrt{6})^n+(2-\sqrt{6})(5-2\sqrt{6})^n], \quad y_n=\frac{1}{2\sqrt{6}}[(2+\sqrt{6})(5+2\sqrt{6})^n-(2-\sqrt{6})(5-2\sqrt{6})^n].$$

Beispiel: Sei $f=1+2x-4x^2y+2y^3-5x^3$ und $X=\{f=0\}$. Durch Probieren findet man $(1,-1)\in X(\mathbf{Z})$. Wie findet man weitere Punkte? Tangentenverfahren: Schneide die Tangente in einem bekannten Punkt mit der Kurve. Die Tangente in $(1,-1)$ ist $f_x(1,-1)(x-1)+f_y(1,-1)(y+1)=0$, d.h. $y=\frac{5}{2}x-\frac{7}{2}$. Eingesetzt in f liefert dies

$$\frac{1}{4}(x-1)^2(65x-339),$$

woraus sich ein weiterer Schnittpunkt der Tangente mit der Kurve berechnet, nämlich $(x_1,y_1)=(\frac{339}{65},\frac{124}{13})$. Iteriert man dies, so erhält man eine Folge rationaler Punkte auf der Kurve:

$$\begin{aligned}
(x_0,y_0) &= (1,-1)\\
(x_1,y_1) &= (\frac{339}{65},\frac{124}{13})\\
(x_2,y_2) &= (-\frac{27392369757513}{66208265164861},-\frac{53999274824480}{66208265164861})\\
x_3 &= \frac{17558528443800805877782634909216083780845798393776339512 89}{2439197458949859721276210357280069140609885262036890179059}\\
y_3 &= \frac{742663701556435033389327381268353861281266237661957409512}{2439197458949859721276210357280069140609885262036890179059}
\end{aligned}$$

Ist h_n der Logarithmus des Zählers von x_n, so findet man

$$h_0=0, h_1=4.17, h_2=31.82, h_3=132.14, h_4=534.55, h_5=2139.84,$$

und

$$\frac{h_2}{h_1} = 7.624, \frac{h_3}{h_2} = 4.152, \frac{h_4}{h_3} = 4.045, \frac{h_5}{h_4} = 4.003.$$

Eine weitere Methode ist die Sekantenmethode: Man schneidet die Verbindungsgerade zweier bekannter Punkte mit der Kurve und erhält einen weiteren Punkt. Tut man dies mit (x_0, y_0) und (x_2, y_2), so erhält man den Punkt

$$\left(\frac{1833818017092291890605}{1079620723098071588773 3}, -\frac{962717965515448813 5001}{1079620723098071588773 3}\right).$$

Transformiert man die Kurve nach einem bei Cassels, S.34/35 beschriebenen Verfahren, so erhält man eine Kurve $y^2 = x^3 - 20000x - 6046875$. APECS transformiert die Kurve in

$$y^2 = x^3 - 32x - 387$$

und bestimmt den Rang zu 1 unter Annahme einiger Vermutungen.

Beispiel: Sei $f = -3 + 3x - 5x^2 + 5xy - 5xy^2$ und $X = \{f = 0\}$. Man sieht schnell $X(\mathbf{Z}/2\mathbf{Z}) = \emptyset$, also auch $X(\mathbf{Z}) = \emptyset$. Was ist mit $X(\mathbf{Q})$?

Beispiel: Sei $f = -5 + x + 2x^4 + 2y^3 + 4y^4$ und $X = \{f = 0\}$. Man findet $(1, -1) \in X(\mathbf{Z})$. Die Menge $X(\mathbf{R})$ ist beschränkt im $\mathbf{R}^2$, woraus sich dann $X(\mathbf{Z}) = \{(1, -1)\}$ ergibt. Was ist $X(\mathbf{Q})$? Das Tangentenverfahren funktioniert hier nicht mehr: die Tangente in $(1, -1)$ ist $y = \frac{9}{10}x - \frac{19}{10}$, einsetzen in f liefert

$$\frac{1}{2500}(x-1)^2(11561x^2 - 28637x + 83526).$$

Ziele bzw. Ergebnisse: Sei $f(x, y) \in \mathbf{Z}[x, y]$ ein *schönes* Polynom vom Grad d und $X = \{f(x, y) = 0\}$. Dann gilt:

- **$d = 3$:** $\#X(\mathbf{Z}) < \infty$ (Siegel 1929). Ist $X(\mathbf{Q}) \neq \emptyset$, so besitzt $X(\mathbf{Q})$ die Struktur einer endlich erzeugten abelschen Gruppe (Mordell 1922).
- **$d \geq 4$:** $\#X(\mathbf{Z}) < \infty$ (Siegel 1929). $\#X(\mathbf{Q}) < \infty$ (Mordell-Vermutung, Faltings 1983).

KAPITEL 2

Algebraische Varietäten

Wir legen im folgenden einen Körper K zugrunde. Sei $\overline{K}$ ein algebraischer Abschluß von K. Wir setzen voraus, daß $\overline{K}$ über K separabel ist. (Ein solcher Körper heißt perfekt.) Dann ist $\overline{K}$ über K galoissch. Sei G_K die Galoisgruppe von $\overline{K}$ über K. Es gilt:

$$K = \{a \in \overline{K} : \sigma a = a \text{ für alle } \sigma \in G_K\}.$$

Algebraisch abgeschlossene Körper, Körper der Charakteristik 0 und endliche Körper sind perfekt.

Affine Varietäten

DEFINITION 1. *Der n-dimensionale affine Raum ist*

$$\mathbf{A}^n = \{P = (a_1, \ldots, a_n) : a_i \in \overline{K}\}.$$

Die Menge der K-rationalen Punkte von $\mathbf{A}^n$ ist

$$\mathbf{A}^n(K) = \{P = (a_1, \ldots, a_n) \in \mathbf{A}^n : a_i \in K\}.$$

Die Galoisgruppe G_K operiert auf $\mathbf{A}^n$ durch $\sigma(a_1, \ldots, a_n) = (\sigma a_1, \ldots, \sigma a_n)$. Dann gilt

$$\mathbf{A}^n(K) = \{P \in \mathbf{A}^n : \sigma P = P \text{ für alle } \sigma \in G_K\}.$$

DEFINITION 2. *Eine Teilmenge $V \subseteq \mathbf{A}^n$ heißt algebraische Menge in $\mathbf{A}^n$, falls es Polynome $f_1, \ldots, f_r \in \overline{K}[x_1, \ldots, x_n]$ gibt mit*

$$V = \{P \in \mathbf{A}^n : f_1(P) = \cdots = f_r(P) = 0\}.$$

Man sagt, eine algebraische Menge V ist über K definiert, falls es Polynome $g_1, \ldots, g_s \in K[x_1, \ldots, x_n]$ gibt mit

$$V = \{P \in \mathbf{A}^n : g_1(P) = \cdots = g_s(P) = 0\}.$$

Man schreibt dann auch V/K. In diesem Fall heißt

$$V(K) = V \cap \mathbf{A}^n = \{P \in K^n : g_1(P) = \cdots = g_s(P) = 0\}$$

die Menge der K-rationalen Punkte von V.

Beispiele: Sei $K = \mathbf{Q}$.

1. Die Beispiele aus dem letzten Abschnitt sind Beispiele für algebraische Mengen in $\mathbf{A}^2$. Sie sind alle über $\mathbf{Q}$ definiert.
2. $V = \{(x, y) \in \mathbf{A}^2 : x^2 - 2y^2 = 0\}$ eine eine über $\mathbf{Q}$ definierte algebraische Menge. Die Menge der $\mathbf{Q}$-rationalen Punkte von V ist $V(\mathbf{Q}) = \{(0, 0)\}$.
3. Die algebraische Menge $V = \{(x, y) \in \mathbf{A}^2 : x - \sqrt{2}y = 0\}$ ist nicht über $\mathbf{Q}$ definiert, wohl aber über $\mathbf{Q}(\sqrt{2})$.
4. Sei $F_d = \{x^d + y^d = 1\}$ und $d \geq 3$. F_d ist über $\mathbf{Q}$ definiert. Die jetzt von Wiles bewiesene Fermatsche Vermutung besagt

$$F_d(\mathbf{Q}) = \{(1, 0), (0, 1)\} \text{ für } d \text{ ungerade }, F_d(\mathbf{Q}) = \{(\pm 1, 0), (0, \pm 1)\} \text{ für } d \text{ gerade.}$$

Ist $X \subseteq \mathbf{A}^n$ über K definiert, d.h. $X = \{f_1 = \cdots = f_r\}$ mit Polynomen $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$, so operiert G_K auf V, denn für $\sigma \in G_K$ gilt:

$$P \in V \Rightarrow f_i(P) = 0 \Rightarrow 0 = \sigma(f_i(P)) = f_i(\sigma(P)) \Rightarrow \sigma(P) \in V.$$

Beispiele:

1. Sei $f = -3y + 2xy + 3y^2$ und $g = 4x + 5y + x^2 + xy$. Dann ist
$$X = \{f = g = 0\} = \{(0,0), (-4,0), (\frac{-5+\sqrt{-35}}{2}, \frac{8-\sqrt{-35}}{3}), (\frac{-5-\sqrt{-35}}{2}, \frac{8+\sqrt{-35}}{3})\}.$$
Die Galoisgruppe $G_{\mathbf{Q}}$ operiert offensichtlich auf X.
2. Sei $f = -3 + 3y + 4x^2 - 5xy$ und $g = -3 - 3x + xy - 5y^2$. Dann ist
$$X = \{f = g = 0\} = \{(-2,-1)\} \cup \{(\alpha, 4\alpha^2 + \alpha - 3) : 20\alpha^3 - 11\alpha^2 - 18\alpha + 12 = 0\}.$$
(Die Galoisgruppe des Polynoms $20x^3 - 11x^2 - 18x + 12$ ist die S_3.)

Definition 3. *Sei $V \subseteq \mathbf{A}^n$ eine algebraische Menge. Dann heißt*
$$I(V) = \{f \in \overline{K}[x_1, \ldots, x_n] : f(P) = 0 \text{ für alle } P \in V\}$$
das Ideal von V. Weiter setzt man
$$I(V/K) = I(V) \cap K[x_1, \ldots, x_n].$$

Bemerkungen:
1. Ist $V = \{f_1 = \cdots = f_r = 0\}$, so verschwinden natürlich auch alle Polynome aus dem Ideal $(f_1, \ldots, f_r)$ auf V. Gibt es noch mehr Polynome? Der Hilbertsche Nullstellensatz besagt, daß
$$I(V) = \sqrt{(f_1, \ldots, f_r)}$$
gilt. Dies setzt die Betrachtung über $\overline{K}$ voraus.
2. Im Polynomring $\overline{K}[x_1, \ldots, x_n]$ gilt
$$I(V/K)\overline{K}[x_1, \ldots, x_n] \subseteq I(V).$$
Gleichheit gilt genau dann, wenn V über K definiert ist.

Definition 4. *Eine algebraische Menge $V \subseteq \mathbf{A}^n$ heißt (absolut) irreduzibel, falls sie nicht als echte Vereinigung weiterer algebraischer Mengen $V_1, V_2 \subseteq \mathbf{A}^n$ geschrieben werden kann, d.h. $V = V_1 \cup V_2$ impliziert $V = V_1$ oder $V = V_2$. Fordert man, daß V, V_1, V_2 über K definiert sind, so nennt man V irreduzibel über K.*

Bemerkung: Sei $f \in K[x_1, \ldots, x_n]$ und $V = \{f = 0\} \subseteq \mathbf{A}^n$. Ist f über K irreduzibel, so ist V über K irreduzibel. Ist f über $\overline{K}$ irreduzibel, so ist V absolut irreduzibel.

Beispiel: $X = \{x^2 = 2y^2\}$ ist über $\mathbf{Q}$ irreduzibel, nicht aber absolut irreduzibel.

Satz 1. *Jede algebraische Menge V ist Vereinigung von endlich vielen irreduziblen:*
$$V = V_1 \cup \cdots \cup V_r.$$
Fordert man noch $V_i \not\subseteq V_j$ für $i \neq j$, so ist diese Darstellung bis auf die Reihenfolge eindeutig. Die V_i's heißen irreduzible Komponenten von V.

Beispiel: Sei $V = \{f = 0\}$ mit $f \in \overline{K}[x_1, \ldots, x_n]$. Da $\overline{K}[x_1, \ldots, x_n]$ ein faktorieller Ring ist, hat man eine (bis auf Konstanten eindeutige) Zerlegung
$$f = f_1^{e_1} \cdots f_r^{e_r},$$
wo die f_i's irreduzible Polynome sind und $e_i \geq 1$. Dann gilt:
$$V = \{f = 0\} = \{f_1 = 0\} \cup \cdots \cup \{f_r = 0\}.$$
Die algebraischen Mengen $\{f_i = 0\}$ sind die irreduziblen Komponenten von V.

Bemerkung: Sei X über K definiert, über K irreduzibel, aber nicht absolut irreduzibel. Sei $V = \{f_1 = \cdots = f_r = 0\}$ eine irreduzible Komponente von X über $\overline{K}$ und für $\sigma \in G_K$
$$V_\sigma = \{\sigma f_1 = \cdots = \sigma f_r = 0\}.$$
Dann gilt
$$X = V_{\sigma_1} \cup \cdots \cup V_{\sigma_s}.$$
$W = V_{\sigma_1} \cap \cdots \cap V_{\sigma_s}$ ist über K definiert und $X(K) \subseteq W(K)$.

Beispiel: $V = \{3 - 3y + x^2 + xy + y^2 = 0\}$ ist über $\mathbf{Q}$ definiert und über $\mathbf{Q}$ irreduzibel. Über $\mathbf{Q}(\sqrt{-3})$ erhält man die Zerlegung

$$V = \{y = \frac{-1+\sqrt{-3}}{2}x + \frac{3+\sqrt{-3}}{2}\} \cup \{y = \frac{-1-\sqrt{-3}}{2}x + \frac{3-\sqrt{-3}}{2}\}.$$

Man sieht dann $V(\mathbf{Q}) = \{(-1,2)\}$.

SATZ 2. *Sei $V \subseteq \mathbf{A}^n$ eine algebraische Menge. V ist genau dann (absolut) irreduzibel, wenn $I(V)$ ein Primideal in $\overline{K}[x_1,\ldots,x_n]$ ist.*

DEFINITION 5. *Eine (absolut) irreduzible Teilmenge von $\mathbf{A}^n$ heißt eine affine Varietät.*

DEFINITION 6. *Sei X eine über K definierte affine Varietät in $\mathbf{A}^n$. Dann heißt*

$$K[X] = K[x_1,\ldots,x_n]/I(V/K)$$

der affine Koordinatenring von V (über K). $K[X]$ ist ein Integritätsring. Sein Quotientenkörper $K(X)$ heißt der Funktionenkörper von V/K.

Interpretation als Funktionen: Sei V eine affine Varietät in $\mathbf{A}^n$. Die Polynome aus $\overline{K}[x_1,\ldots,x_n]$ können wir als Funktionen $V \to \overline{K}$ betrachten. Für zwei Polynome f,g gilt: f und g liefern genau dann die gleiche Funktion auf V, wenn $f-g$ auf V verschwindet, d.h. wenn $f-g \in I(V)$ gilt, anders ausgedrückt: $f \equiv g \bmod I(V)$. Die Elemente aus $\overline{K}[V]$ können also als Funktionen auf V betrachtet werden.

DEFINITION 7. *Sei $V \subseteq \mathbf{A}^n$ eine Varietät. Dann wird die Dimension von V definiert als*

$$\dim V = \max\{n : V_0 \subset V_1 \subset \cdots \subset V_n = V, V_i \textit{ irreduzibel}\}.$$

Bemerkung: Die Dimension von V berechnet sich auch als Transzendenzgrad von $\overline{K}(V)$ über $\overline{K}$.

Beispiele:

1. $\overline{K}[\mathbf{A}^n] = \overline{K}[x_1,\ldots,x_n]$.
2. Sei $f \in \overline{K}[x_1,\ldots,x_n]$ ein irreduzibles Polynom. Dann ist $V = \{f = 0\}$ eine Varietät der Dimension $n-1$. Außerdem gilt
$$\overline{K}[V] = \overline{K}[x_1,\ldots,x_n]/(f).$$

DEFINITION 8. *Sei $V \subseteq \mathbf{A}^n$ eine Varietät, $I(V) = (f_1,\ldots,f_r)$ und $P \in V$. Man sagt V ist nichtsingulär (oder glatt) in P, falls gilt*

$$\dim V = n - Rang((\frac{\partial f_i}{\partial x_j})_{i,j}).$$

Ist V in jedem Punkt nichtsingulär, so heißt V nichtsingulär.

Beispiel: Sei $f(x,y) \in \overline{K}[x,y]$ ein irreduzibles Polynom. Dann ist $V = \{f = 0\}$ eine 1-dimensionale affine Varietät, eine Kurve. V ist genau dann nichtsingulär in $P \in V$, wenn

$$(f_x(P), f_y(P)) \neq 0.$$

Dann ist $f_x(P)(x - x_P) + f_y(P)(y - y_P) = 0$ die Tangente in $P = (x_P, y_P)$.

Beispiel: $y^2 = x^2 + x^3$ und $y^2 = x^3$ sind jeweils singulär in $(0,0)$.

DEFINITION 9. *Sei V eine affine Varietät und $P \in V$. Dann heißt*

$$\overline{K}[V]_P = \{\frac{f}{g} \in \overline{K}(V) : f,g \in \overline{K}[V], g(P) \neq 0\}$$

der lokale Ring von V in P.

Der lokale Ring von V in P besteht also aus den Funktionen des Funktionenkörpers, die in P definiert sind. Offensichtlich gilt:

$$\overline{K}[V] \subseteq \overline{K}[V]_P \subseteq \overline{K}(V).$$

Beispiele:

1. Wir wissen bereits $K[\mathbf{A}^2] = K[x,y]$ und
$$K(\mathbf{A}^2) = K(x,y) = \{\frac{f(x,y)}{g(x,y)} : f,g \in K[x,y]\}.$$
Für $P = (2,-1)$ gilt dann
$$K[\mathbf{A}^2]_P = \{\frac{f(x,y)}{g(x,y)} : f,g \in K[x,y], g(2,-1) \neq 0\}.$$
2. Sei $X = \{y^2 = x^3\} \subseteq \mathbf{A}^2$. Dann ist $K[X] = K[x,y]/(y^2 - x^3)$. Jedes Element aus $K[X]$ hat die Gestalt $a(x) + b(x)y$ mit Polynomen $a,b \in K[x]$. Wir betrachten die Funktion $f = \frac{y}{x}$. Sie ist definiert für alle $P \neq (0,0)$. Für f^2 gilt im Funktionenkörper:
$$f^2 = \frac{y^2}{x^2} = \frac{x^2 + x^3}{x^2} = 1 + x,$$
also ist f^2 in allen Punkten definiert, auch in $(0,0)$.

Projektive Varietäten

Vorbemerkung: Um die rationalen Lösungen der Gleichung $f = 2x^2 + 3y^2 - 1 = 0$ zu bestimmen, hatten wir substituiert $x = \frac{X}{Z}, y = \frac{Y}{Z}$ und die Gleichung $g = 2X^2 + 3Y^2 - Z^2$ erhalten. Mit (X_0, Y_0, Z_0) erfüllt auch $(\lambda X_0, \lambda Y_0, \lambda Z_0)$ die Gleichung $g = 0$ für jedes λ. Dies entspricht dem Übergang vom Affinen zum Projektiven.

Definition 10. *Auf $\mathbf{A}^{n+1} \setminus \{(0,\dots,0)\}$ wird durch*
$$(x_0,\dots,x_n) \sim (y_0,\dots,y_n) \iff x_i = \lambda y_i \text{ für ein } \lambda \in \overline{K}^\times \text{ und alle } i$$
eine Äquivalenzrelation definiert. Die Äquivalenzklasse von $(x_0,\dots,x_n)$ wird mit $(x_0 : \dots : x_n)$ bezeichnet. Die x_i's heißen homogene Koordinaten von $(x_0 : \dots : x_n)$. Die Menge der Äquivalenzklassen heißt n-dimensionaler projektiver Raum (über K):
$$\mathbf{P}^n = \mathbf{P}^n(\overline{K}) = \{(x_0 : \dots : x_n) : x_i \in \overline{K}, (x_0,\dots,x_n) \neq 0\}.$$
Die Menge der K-rationalen Punkte von $\mathbf{P}^n$ ist
$$\mathbf{P}(K) = \{(x_0 : \dots : x_n) \in \mathbf{P}^n : x_i \in K\}.$$

Beispiel: Wie stellt man sich projektive Räume vor?
$$\mathbf{P}^1 = \{(1 : x) : x \in \overline{K}\} \cup \{(0 : 1)\}$$
sieht aus wie eine affine Gerade mit einem (unendlich fernen) Punkt.
$$\mathbf{P}^2 = \{(1 : x : y) : x,y \in \overline{K}\} \cup \{(0 : z_0 : z_1)\}$$
sieht aus wie eine affine Ebene mit einer (unendlich fernen) projektiven Geraden.

Beispiel: Es gilt
$$\mathbf{P}^n(\mathbf{Q}) = \{(a_0 : \dots : a_n) : a_i \in \mathbf{Z}, ggT(a_0,\dots,a_n) = 1\}.$$

Bemerkung: Aus $P = (x_0 : \dots : x_n) \in \mathbf{P}^n(K)$ folgt noch nicht $x_i \in K$, wie das Beispiel $(0 : \sqrt{2}) = (0 : 1) \in \mathbf{P}^1(\mathbf{Q})$ zeigt. Dies ändert sich, wenn man eine der homogenen Koordinaten zu 1 normiert. Ist $P = (x_0 : \dots : x_n) \in \mathbf{P}^n(\overline{K})$ und $x_i \neq 0$, so nennt man
$$K(P) = K(\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}) (\subseteq \overline{K})$$
den minimalen Definitionskörper von P über K. Die Galoisgruppe operiert natürlich auch auf $\mathbf{P}^n(\overline{K})$ und man sieht schnell
$$\mathbf{P}^n(K) = \{P \in \mathbf{P}^n : \sigma P = P \text{ für alle } \sigma \in G_K\}$$
und
$$K(P) = \text{ Fixkörper von } \{\sigma \in G_K : \sigma P = P\}.$$

Vorbemerkung: Wir wollen nun algebraische Teilmengen im $\mathbf{P}^n$ definieren als Nullstellenmenge von Polynomen. Ist f ein Polynom und $P = (a_0 : \dots : a_n) \in \mathbf{P}^n$, so wollen wir haben

$$f(a_0, \dots, a_n) = 0 \iff f(\lambda a_0, \dots, \lambda a_n) = 0$$

für alle $\lambda \in \overline{K}$. Diese Bedingung wird von homogenen Polynomen erfüllt: $f(x_0, \dots, x_n)$ heißt homogen vom Grad d, falls gilt

$$f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n).$$

Äquivalent dazu ist, daß in f nur Monome vom Grad d auftreten, d.h. f hat die Form

$$f = \sum_{i_0 + \dots + i_n = d} a_{i_0 \dots i_n} x_0^{i_0} \dots x_n^{i_n}.$$

Definition 11. *Eine Teilmenge $V \subseteq \mathbf{P}^n$ heißt algebraische Teilmenge in $\mathbf{P}^n$, falls es homogene Polynome $f_1, \dots, f_r \in \overline{K}[x_0, \dots, x_n]$ gibt mit*

$$V = \{P \in \mathbf{P}^n : f_1(P) = \dots = f_r(P) = 0\} = \{f_1 = \dots = f_r = 0\}.$$

Man sagt, die algebraische Menge $V \subseteq \mathbf{P}^n$ ist über K definiert, falls es Polynome $g_1, \dots, g_s \in K[x_0, \dots, x_n]$ gibt mit $V = \{g_1 = \dots = g_s = 0\}$. In diesem Fall heißt

$$V(K) = V \cap \mathbf{P}^n(K)$$

die Menge der K-rationalen Punkte von V.

Genau wie im affinen Fall definiert man, wann eine algebraische Teilmenge irreduzibel heißt.

Definition 12. *Eine projektive Varietät ist eine irreduzible algebraische Menge in einem $\mathbf{P}^n$.*

Das Ideal $I(V)$ einer algebraischen Menge $V \subseteq \mathbf{P}^n$ ist das Ideal, das von allen homogenen Polynomen $f \in \overline{K}[x_0, \dots, x_n]$ erzeugt wird, die auf V verschwinden. Dann gilt:

$$V \subseteq \mathbf{P}^n \text{ ist projektive Varietät} \iff I(V) \text{ ist Primideal.}$$

Wieder kann man jede algebraische Teilmenge des $\mathbf{P}^n$ in eine endliche Vereinigung von irreduziblen Komponenten zerlegen.

Zariski-Topologie:

- Sind $V = \{f_1 = \dots = f_r = 0\}$ und $W = \{g_1 = \dots = g_s = 0\}$ algebraische Mengen, so auch
$$V \cup W = \{f_1 g_1 = \dots = f_1 g_s = \dots = f_r g_1 = \dots = f_r g_s = 0\}.$$
- Seien $V_i = \{f_{i1} = \dots = f_{ir_i} = 0\}$, $i \in I$ algebraische Mengen. Nach dem Hilbertschen Basissatz ist das Ideal $(f_{ij} : i \in I, 1 \le j \le r_i)$ endlich erzeugt, d.h. es gibt Polynome $g_1, \dots, g_s$ mit $(f_{ij} : i \in I, 1 \le j \le r_i) = (g_1, \dots, g_s)$ und damit
$$\cap_{i \in I} V_i = \{P \in \mathbf{P}^n : f_{ij}(P) = 0 \text{ für alle } i \in I \text{ und alle } j = 1, \dots, r_i\} = \{g_1 = \dots = g_s = 0\}.$$
Also ist auch $\cap_{i \in I} V_i$ eine algebraische Menge.
- Weiter sind $\emptyset = \{1 = 0\}$ und $\mathbf{P}^n = \{0 = 0\}$ algebraische Mengen.

Die algebraischen Teilmengen des $\mathbf{P}^n$ erfüllen damit die Aximome für die abgeschlossenen Teilmengen einer Topologie. Man nennt diese Topologie die Zariski-Topologie auf dem $\mathbf{P}^n$. (Das gleiche gilt natürlich auch auf dem $\mathbf{A}^n$.) Damit können wir jetzt topologische Begriffe verwenden. Teilmengen des $\mathbf{P}^n$ denken wir uns mit der induzierten Topologie versehen. Daß diese Topologie etwas ungewöhnlich ist, zeigen folgende Beispiele:

Beispiel: Sei $X \subseteq \mathbf{P}^n$ eine projektive Varietät und $U, V \subseteq X$ zwei offene nichtleere Teilmengen von X. Dann gilt $U \cap V \neq \emptyset$.
Beweis: Wäre $U \cap V = \emptyset$, so hätte man

$$X = (X \setminus U) \cup (X \setminus V).$$

$X \setminus U$ und $X \setminus V$ sind abgeschlossene Mengen von X, also algebraische Mengen des $\mathbf{P}^n$. Da X irreduzibel ist, folgt $X = X \setminus U$ oder $X = X \setminus V$, d.h. $U = \emptyset$ oder $V = \emptyset$, ein Widerspruch zur Voraussetzung. ■

Beispiel: Die abgeschlossenen Teilmengen des $\mathbf{P}^1$ sind $\emptyset$, $\mathbf{P}^1$ und alle endlichen Teilmengen.

Wir wollen nun den $\mathbf{P}^n$ betrachten. Sei $0 \le i \le n$ gegeben. Dann ist $H_i = \{x_i = 0\}$ abgeschlossen und $U_i = \mathbf{P}^n \setminus H_i = \{x_i \neq 0\}$ offen in $\mathbf{P}^n$. Für $(x_0 : \cdots : x_n) \in U_i$ gilt:

$$(x_0 : \cdots : x_{i-1} : x_i : x_{i+1} : \cdots : x_n) = (\frac{x_0}{x_i} : \cdots : \frac{x_{i-1}}{x_i} : 1 : \frac{x_{i+1}}{x_i} : \cdots : \frac{x_n}{x_i}).$$

Definiert man also

$$\phi_i : \mathbf{A}^n \to U_i, \quad (y_1, \ldots, y_n) \mapsto (y_1 : \cdots : y_{i-1} : 1 : y_{i+1} : \cdots : y_n)$$

und

$$\psi_i : U_i \to \mathbf{A}^n, \quad (x_0 : \cdots : x_{i-1} : x_i : x_{i+1} : \cdots : x_n) \mapsto (\frac{x_0}{x_i} : \cdots : \frac{x_{i-1}}{x_i} : \frac{x_{i+1}}{x_i} : \cdots : \frac{x_n}{x_i}),$$

so sind ϕ_i und ψ_i invers zueinander. Wir können also $\mathbf{A}^n$ als offene Teilmenge des $\mathbf{P}^n$ betrachten. Oft wählen wir $i = 0$, d.h. wir denken uns $\mathbf{A}^n \subset \mathbf{P}^n$ mit $(x_1, \ldots, x_n) \simeq (1 : x_1 : \cdots : x_n)$.

Ist $V \subseteq \mathbf{P}^n$ eine projektive algebraische Menge, gegeben durch

$$V = \{f_1(x_0, \ldots, x_n) = \cdots = f_r(x_0, \ldots, x_n) = 0\},$$

wo die f_i's homogene Polynome sind, so ist $V \cap \mathbf{A}^n$ eine affine algebraische Menge, gegeben durch die Gleichungen

$$V \cap \mathbf{A}^n = \{f_1(1, x_1, \ldots, x_n) = \cdots = f_r(1, x_1, \ldots, x_n) = 0\}.$$

Wichtiger ist die Umkehrung:

Definition 13. *Ist $V \subseteq \mathbf{A}^n$ eine affine algebraische Menge, so denken wir uns V mit $V \subseteq \mathbf{A}^n \subset \mathbf{P}^n$ als Teilmenge des $\mathbf{P}^n$. Der topologische Abschluß $\overline{V}$ von V in $\mathbf{P}^n$ heißt der projektive Abschluß von V.*

Wie berechnet man den projektiven Abschluß? Dazu brauchen wir das Homogenisieren von Polynomen. Sei $f(x_1, \ldots, x_n) \in \overline{K}[x_1, \ldots, x_n]$ ein Polynom vom Grad d. Das homogenisierte Polynom ist dann

$$f^*(x_0, \ldots, x_n) = x_0^d f(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}).$$

Man kann dies auch explizit ausschreiben: Ist

$$f = \sum_{i_1 + \cdots + i_n \le d} a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n},$$

so ist

$$f^* = \sum_{i_0 + i_1 + \cdots + i_n = d} a_{i_1 \ldots i_n} x_0^{i_0} x_1^{i_1} \ldots x_n^{i_n}.$$

Damit gilt nun: Ist die affine algebraische Menge V gegeben durch die Gleichungen $V = \{f_1 = \cdots = f_r = 0\}$, so ist der projektive Abschluß von V gegeben durch

$$\overline{V} = \{f_1^* = \cdots = f_r^* = 0\}.$$

Ohne Beweis geben wir folgenden Satz an:

Satz 3.
1. *Ist V eine affine Varietät, so ist $\overline{V}$ eine projektive Varietät und $V = \overline{V} \cap \mathbf{A}^n$. Ist V über K definiert, so auch $\overline{V}$.*
2. *Ist W eine projektive Varietät, so ist entweder $W \cap \mathbf{A}^n = \emptyset$ oder $W \cap \mathbf{A}^n$ eine affine Varietät und $W = \overline{W \cap \mathbf{A}^n}$. Ist W über K definiert, so auch $W \cap \mathbf{A}^n$.*

Auf diese Weise definiert jede affine Varietät eindeutig eine projektive Varietät. Oft werden wir projektive Varietäten V durch affine Gleichungen angeben, weil dies etwas einfacher aussieht. Die Punkte $V \cap H_0$ heißen auch unendlich ferne Punkte der Varietät.

Beispiel: Sei $X \subseteq \mathbf{P}^2$ gegeben durch $y = x^2$. Homogenisieren liefert $x_0 x_2 = x_1^2$. Es gibt einen unendlich fernen Punkt, nämlich $(0 : 0 : 1)$. Betrachtet man X im affinen Teil $x_1 \neq 0$, so kann man setzen $(x_0 : x_1 : x_2) = (u : 1 : v)$ und man erhält die Gleichung $uv = 1$. Parabel und Hyperbel sind also nur verschiedene affine Ansichten der gleichen projektiven Kurve.

Beispiel: Eine Gerade im $\mathbf{A}^2$ wird gegeben durch eine Gleichung $ax + by + c = 0$ mit $a, b, c \in K$, $(a, b) \neq (0, 0)$. Der projektive Abschluß davon ist $ax_1 + bx_2 + cx_0 = 0$. Dies ist eine Gerade in $\mathbf{P}^2$. Ist

$a = b = 0$, so erhält man die unendlich ferne Gerade $x_0 = 0$. Zwei Geraden im $\mathbf{P}^2$ schneiden sich immer. Wo schneiden sich $y = ax + b_1$ und $y = ax + b_2$, falls $b_1 \neq b_2$ ist? Homogen lauten die Gleichungen

$$x_2 = ax_1 + b_1 x_0 \text{ und } x_2 = ax_1 + b_2 x_0,$$

woraus sich als Schnittpunkt $(0 : 1 : a)$ berechnet. Er liegt auf der unendlich fernen Geraden.

Die Dimension einer projektiven Varietät wird definiert wie im affinen Fall.

Definition 14. *Sei V/K eine projektive Varietät. Wähle $\mathbf{A}^n \subseteq \mathbf{P}^n$ mit $V \cap \mathbf{A}^n \neq \emptyset$. Der Funktionenkörper von V wird definiert als*

$$K(V) = K(V \cap \mathbf{A}^n).$$

(Eine andere Wahl von $\mathbf{A}^n \subseteq \mathbf{P}^n$ liefert kanonisch isomorphe Körper.)

Bemerkung: Man kann den Funktionenkörper $K(V)$ einer projektiven Varietät auch noch etwas anders definieren, nämlich als Menge aller Quotienten $\frac{f(x_0,\dots,x_n)}{g(x_0,\dots,x_n)}$ homogener Polynome gleichen Grades mit $g \notin I(V)$ und der Relation $\frac{f_1}{g_1} = \frac{f_2}{g_2}$ genau dann, wenn $f_1 g_2 - f_2 g_1 \in I(V)$.

Beispiel: Wie sieht der Funktionenkörper des $\mathbf{P}^1$ aus? Setzt man $(x_0 : x_1) = (1 : t) = (u : 1)$, so ist ein $\phi \in K(\mathbf{P}^1)$ eine rationale Funktion $\phi = \frac{f(t)}{g(t)}$ mit Polynomen $f, g \in K[t]$. Wegen $u = \frac{1}{t}$ hat ϕ auch die Darstellung

$$\phi = \frac{f(t)}{g(t)} = \frac{f(\frac{1}{u})}{g(\frac{1}{u})}.$$

Oder homogen:

$$\phi = \frac{f(\frac{x_1}{x_0})}{g(\frac{x_1}{x_0})}.$$

Definition 15. *Sei V eine projektive Varietät und $P \in V$. Wähle $\mathbf{A}^n \subseteq \mathbf{P}^n$ mit $P \in \mathbf{A}^n$. (Dann ist $V \cap \mathbf{A}^n$ eine offene Umgebung von P in V.)*

1. *P heißt singulärer Punkt von V, falls P singulärer Punkt von $V \cap \mathbf{A}^n$ ist; andernfalls nichtsingulär oder glatt.*
2. *Der lokale Ring von V in $P \in V$ ist der lokale Ring von $V \cap \mathbf{A}^n$ in P. Er besteht aus allen Funktionen aus $\overline{K}(V)$, die in P definiert sind.*

Bemerkung: Ist $X = \{f(x_0, \dots, x_n) = 0\} \subseteq \mathbf{P}^n$, wo f ein irreduzibles homogenes Polynom ist, so ist die Menge der Singularitäten von X gegeben durch

$$X_{sing} = \{f = \frac{\partial f}{\partial x_0} = \dots = \frac{\partial f}{\partial x_n} = 0\}.$$

Für homogene Polynome gilt die Eulersche Relation

$$d \cdot f = \sum_{i=0}^{n} x_i \frac{\partial f}{\partial x_i},$$

wenn d der Grad von f ist. Hat also d nichts mit der Charakteristik von K zu tun, so kann man auf die Gleichung f in X_{sing} verzichten.

Der folgende Satz gibt einen fundamentalen Unterschied zwischen affinen und projektiven Varietäten an:

Satz 4.
1. *Ist $V \subseteq \mathbf{A}^n$ eine affine Varietät und $f \in \overline{K}(V)$ eine Funktion, die in allen Punkten $P \in V$ definiert ist, dann ist $f \in \overline{K}[V]$.*
2. *Ist $W \subseteq \mathbf{P}^n$ eine projektive Varietät und $g \in \overline{K}(V)$ eine Funktion, die in allen Punkten $P \in W$ definiert ist, dann gilt $g \in \overline{K}$.*

Produkte von Varietäten

Was sind die algebraischen Teilmengen von $\mathbf{P}^m \times \mathbf{P}^n$?

Definition 16. *Ein Polynom $f \in \overline{K}[x_0, \ldots, x_m, y_0, \ldots, y_n]$ heißt bihomogen vom Grad (d.e) bzgl. $x_0, \ldots, x_m$ und $y_0, \ldots, y_n$, wenn es die Gestalt*

$$f = \sum_{i_0+\cdots+i_m=d} \sum_{j_0+\cdots+j_n=e} a_{i_0\ldots i_m j_0\ldots j_n} x_0^{i_0} \ldots x_m^{i_m} y_0^{j_0} \ldots y_n^{j_n}$$

hat. D.h. f ist homogen vom Grad d in den Variablen x_i und homogen vom Grad e in den Variablen y_j.

Definition 17. *Auf $\mathbf{P}^m \times \mathbf{P}^n$ nennen wir eine Menge abgeschlossen oder algebraisch, falls sie Nullstellenmenge bihomogener Polynome $f_\ell(x, y)$ ist. Dies induziert eine Topologie, die wir wieder Zariski-Topologie nennen.*

Bemerkungen:

1. Analog werden Produkte zwischen projektiven und affinen Varietäten definiert.
2. Die Zariski-Topologie auf $\mathbf{P}^m \times \mathbf{P}^n$ ist nicht die Produkttopologie.

Abbildungen zwischen Varietäten

Definition 18. *Seien V und W projektive Varietäten, $W \subseteq \mathbf{P}^n$. Eine rationale Abbildung $\phi : V \to W$ wird gegeben durch Funktionen $f_i \in \overline{K}(V)$, nicht alle 0, durch $\phi = (f_0 : \cdots : f_n)$ mit der Eigenschaft $F(f_0, \ldots, f_n) = 0$ für alle $F \in I(W)$. ϕ heißt definiert in $P \in V$, falls es eine Funktion $g \in \overline{K}$ gibt mit der Eigenschaft:*

- *Alle gf_i sind definiert in P,*
- *für mindestens ein i ist $(gf_i)(P) \neq 0$.*
- *Dann setzt man*

$$\phi(P) = ((gf_0)(P) : \cdots : (gf_n)(P)).$$

Sind V und W über K definiert, so heißt ϕ definiert über K, falls die $f_i \in K(V)$ gewählt werden können.

Beispiel: Wir betrachten $X \subseteq \mathbf{P}^2$ gegeben durch die Gleichung $2x^2 + 3y^2 - 5 = 0$, d.h.

$$X = \{2x_1^2 + 3x_2^2 = 5x_0^2\}.$$

Affine Koordinaten führen wir ein durch

$$(x_0 : x_1 : x_2) = (1 : x : y) = (u : 1 : v).$$

Dann sind $x, y, u, v \in K(X)$ und $x = \frac{1}{u}, y = \frac{v}{u}$. Wir definieren die rationale Abbildung $\phi : X \to \mathbf{P}^1$ durch

$$\phi = (1 : \frac{y-1}{x-1}).$$

Wegen $\phi = (x - 1 : y - 1)$ ist ϕ sicher definiert in der offenen Menge $\{x_0 \neq 0\} \setminus \{(1 : 1 : 1)\}$. Wegen $\phi = (1 - u : v - u)$ ist ϕ auch in der offenen Menge $\{x_1 \neq 0\} \setminus \{(1 : 1 : 1)\}$ definiert. Es bleibt jetzt nur noch das Verhalten im Punkt $(1 : 1 : 1)$ zu untersuchen. Im Funktionenkörper $K(X)$ gilt $2x^2 + 3y^2 = 5$ und damit $3(y^2 - 1) = -2(x^2 - 1)$, was sofort

$$\frac{y-1}{x-1} = -\frac{2}{3}\frac{x+1}{y+1}$$

liefert. Damit ist ϕ auch in $(1 : 1 : 1)$ definiert mit Wert $(1 : -\frac{2}{3})$.

Beispiel: Sei $X \subseteq \mathbf{P}^2$ definiert durch $y^2 = x^3$, d.h. $X = \{x_0 x_2^2 = x_1^3\}$. Wir definieren eine rationale Abbildung $\phi : X \to \mathbf{P}^1$ durch $\phi = (1 : \frac{y}{x})$. Schreibt man

$$\phi = (1 : \frac{y}{x}) = (x : y) = (x_1 : x_2),$$

dann sieht man, daß ϕ außerhalb des Punktes $(0, 0$ definiert ist. Wir wollen untersuchen, was in diesem Punkt passiert.

- Zunächst ist schnell klar, daß gilt, daß sich jedes Element des Funktionenkörpers als $\frac{a(x)+b(x)y}{c(x)}$ schreiben läßt. Wählt man a, b, c teilerfremd, so ist diese Darstellung eindeutig.

- Sei $f = \frac{a+by}{c}$ gekürzt dargestellt. f ist genau dann in P definiert, falls $c(0) \neq 0$ ist.
- Angenommen, ϕ wäre auch in $(0,0)$ definiert. Dann gäbe es ein g im Funktionenkörper, so daß g und $g\frac{y}{x}$ in $(0,0)$ definiert sind und dort nicht beide den Wert 0 haben. Wir können also schreiben $g = \frac{a+by}{c}$ mit $c(0) \neq 0$. Dann hat man
$$g\frac{y}{x} = \frac{ay+by^2}{xc} = \frac{x^3b+ay}{xc}.$$
Da dies in $(0,0)$ definiert sein soll, ist $a(0)=0$, d.h. $a = xd$ mit einem Polynom d. Dann gilt:
$$g = \frac{xd+by}{c}, \quad g\frac{y}{x} = \frac{x^2b+y}{c}.$$
Beide sind in $(0,0)$ definiert, aber beide nehmen den Wert 0 an, ein Widerspruch.

Also ist ϕ in $(0,0)$ nicht definiert.

Bemerkung: Seien V, W projektive Varietäten, die über K definiert, und $\phi : V \to W$ eine rationale Abbildung gegeben durch $\phi = (f_0 : \cdots : f_n)$. Dann operiert G_K auf ϕ durch $\sigma\phi = (\sigma f_0 : \cdots : \sigma f_n)$. Genau dann ist ϕ über K definiert, falls $\sigma\phi = \phi$ für alle $\sigma \in G_K$ gilt.

Bemerkung: Da wir uns die Elemente des Funktionenkörpers auch als Quotienten homogener Polynome gleichen Grades vorstellen können, können wir auch schreiben
$$\phi = (g_0(x_0,\ldots,x_m) : \cdots : g_n(x_0,\ldots,x_m)),$$
wo g_i homogene Polynome gleichen Grades sind, aber nicht alle in $I(V)$ liegen.

Beispiel: Wir betrachten die rationale Abbildung $\phi : \mathbf{P}^2 \to \mathbf{P}^1$, die durch $\phi = (x : y)$ gegeben ist. Schreiben wir $x = \frac{x_1}{x_0}, y = \frac{x_2}{x_0}$, so wird $\phi = (x_1 : x_2)$. ϕ ist in allen Punkten von $\mathbf{P}^2$ außer in $(1:0:0)$ definiert. Was passiert geometrisch? Die Geraden durch $(1:0:0)$ haben die Gestalt $x_2 = \lambda x_1$ oder $x_1 = 0$. Was macht ϕ mit den Punkten? Ein Punkt auf $x_2 = \lambda x_1$ wird abgebildet auf $(1:\lambda)$, ein Punkt auf $x_1 = 0$ auf $(0:1)$. Es ist klar, daß ϕ in $(1:0:0)$ nicht definiert werden kann.

Beispiel: (Projektionen) Eine rationale Abbildung der Form
$$\mathbf{P}^n \to \mathbf{P}^{n-1}, \quad (x_0 : \cdots : x_n) \mapsto (x_0 : \cdots : x_{n-1})$$
nennt man Projektion.

LEMMA 1. *Sei $\phi : V \to W$ eine rationale Abbildung zwischen projektiven Varietäten. Dann ist $U = \{P \in V : \phi$ definiert in $P\}$ eine offene Teilmenge von V.*

Beweis: Sei $P \in U$ und $\phi = (f_0 : \cdots : f_n)$, wo f_i homogene Polynome sind, mit $f_j(P) \neq 0$. Dann ist ϕ dadurch auch in der offenen Umgebung $\{f_j \neq 0\} \cap V$ von P definiert, woraus sofort die Behauptung folgt. ■

DEFINITION 19.
1. *Eine rationale Abbildung $\phi : V \to W$ zwischen projektiven Varietäten heißt Morphismus, wenn ϕ in allen Punkten von V definiert ist.*
2. *Ein Morphismus $\phi : V \to W$ heißt Isomorphismus, falls es einen Morphismus $\psi : W \to V$ gibt, so daß $\phi\psi$ und $\psi\phi$ jeweils die Identität sind.*
3. *Sind V und W über K definiert, so heißen V und W über K isomorph, falls über K definierte Morphismen $\phi : V \to W$ und $\psi : W \to V$ existieren, so daß $\phi\psi$ und $\psi\phi$ jeweils die Identität sind.*

Bemerkung: Da wir affine Varietäten projektiv abschließen können, ist klar, wie man rationale Abbildungen und Morphismen auch für affine Varietäten definiert.

Projektiver Koordinatenwechsel: Sei $T \in GL_{n+1}(\overline{K})$. Dann induziert T eine lineare Abbildung des $\overline{K}^{n+1}$, die einen Automorphismus des $\mathbf{P}^n$ liefert. Man nennt dies einen Koordinatenwechsel. Zwei Teilmengen des $\mathbf{P}^n$ heißen projektive äquivalent, wenn sie durch einen Koordinatenwechsel auseinander hervorgehen.

Für die diophantische Geometrie ist folgender Satz wichtig:

SATZ 5. *Sind V und W über K definierte projektive Varietäten und $\phi : V \to W$ ein über K definierter Isomorphismus, so induziert ϕ eine Bijektion $V(K) \simeq W(K)$.*

Beweis: ϕ und ϕ^{-1} können also durch Polynome beschrieben werden, die Koeffizienten in K haben. Natürlich werden dann Punkte von $V(K)$ und $W(K)$ ineinander abgebildet. Da aber ϕ bijektiv ist, folgt die Behauptung. ■

Bemerkungen:

1. Man könnte also eine Aufgabe der diophantischen Geometrie so formulieren: Klassifiziere über K-definierte projektive Varietäten bis auf K-Isomorphie und bestimme jeweils die K-rationalen Punkte.
2. Ein erster Schritt dazu ist ein Ziel der algebraischen Geometrie: Klassifiziere projektive Varietäten bis auf Isomorphie, wobei hier alles über algebraisch abgeschlossenem Körper zu sehen ist. Allerdings ist auch diese Aufgabe noch zu schwierig.

Beispiel: Sei $X_n \subseteq \mathbf{P}^2$ definiert durch die affine Gleichung $2x^2 + 3y^2 = n$. Also $X_n = \{2x_1^2 + 3x_2^2 = nx_0^2\}$. Offensichtlich gilt

$$X_n(\mathbf{Q}) = \{(1 : x : y) : 2x^2 + 3y^2 = n \text{ und } x, y \in \mathbf{Q}\}.$$

Wir haben gesehen: $X_1(\mathbf{Q}) = \emptyset$ und $\#X_5(\mathbf{Q}) = \infty$, also sind X_1 und X_5 nicht über $\mathbf{Q}$ isomorph. Andererseits induziert der Koordinatenwechsel

$$\phi((x_0 : x_1 : x_2)) = (\sqrt{5}x_0 : x_1 : x_2)$$

einen Isomorphismus von X_1 mit X_5, der über $\mathbf{Q}(\sqrt{5})$ definiert ist.

Folgendes Beispiel rechne man als Übungsaufgabe:

Beispiel: Im $\mathbf{P}^2$ sei eine Quadrik Q gegeben durch die affine Gleichung $y + ax^2 + bxy + cy^2 = 0$ mit $a \neq 0$. Man zeige:

1. Q ist irreduzibel.
2. Die rationale Abbildung $\phi : X \to \mathbf{P}^1$ mit
$$\phi = (1 : \frac{y}{x})$$
ist ein Morphismus.
3. Die rationale Abbildung $\psi' : \mathbf{P}^1 \to \mathbf{P}^2$ mit
$$\psi' = (1 : -\frac{t}{a + bt + ct^2} : -\frac{t^2}{a + bt + ct^2})$$
ist ein Morphismus und induziert einen Morphismus $\psi : \mathbf{P}^1 \to X$.
4. ϕ und ψ sind invers zueinander, d.h. $X \simeq \mathbf{P}^1$.

Von fundamentaler Bedeutung ist folgender Satz, den wir nicht beweisen werden:

SATZ 6. *Ist X eine projektive Varietät und $\phi : X \to \mathbf{P}^n$ ein Morphismus, so ist $\phi(X)$ abgeschlossen, d.h. $\phi(X)$ läßt sich in $\mathbf{P}^n$ durch Gleichungen beschreiben.*

Daß dies Aussage i.a. für affine Varietäten nicht gilt, zeigt folgendes Beispiel:

Beispiel:

1. Wir betrachten die affine Varietät $X = \{(x, y) \in \mathbf{A}^2 : xy = 1\}$ und den Morphismus $\phi : X \to \mathbf{A}^1$ mit $\phi((x, y)) = x$. Offensichtlich ist $\phi(X) = \mathbf{A}^1 \setminus \{0\}$ keine abgeschlossenen Teilmenge von $\mathbf{A}^1$.
2. Dies wird auch nicht anders, wenn man $\phi : X \to \mathbf{P}^1$ mit $\phi((x, y)) = (1 : x)$ betrachtet. Dann ist $\phi(X) = \mathbf{P}^1 \setminus \{(1 : 0), (0 : 1)\}$, auch keine abgeschlossene Teilmenge von $\mathbf{P}^1$.

3. Wir betrachten jetzt den projektiven Abschluß von X im $\mathbf{P}^2$: $Y = \{(x_0 : x_1 : x_2) \in \mathbf{P}^2 : x_1x_2 = x_0^2\}$. Wir haben die 2 Punkte $(0:1:0)$ und $(0:0:1)$ dazu bekommen. Die rationale Abbildung $\phi : Y \to \mathbf{P}^1$ mit
$$\phi = (1 : x) = (1 : \frac{x_1}{x_0}) = (x_0 : x_1) = (x_0^2 : x_0x_1) = (x_2 : x_0)$$
ist ein Morphismus, wie man an den verschiedenen Darstellungen sieht und $\phi((0:1:0)) = (0:1)$, $\phi((0:0:1)) = (1:0)$. Damit folgt sofort $\phi(Y) = \mathbf{P}^1$, insbesondere ist $\phi(Y)$ abgeschlossen.

Wie obiges Ergebnis angewendet werden kann, zeigt folgendes Beispiel:

Beispiel: Ebene Quadriken werden definiert durch eine Gleichung
$$f_{(a_0,\dots,a_5)} = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = 0.$$
Natürlich kann man die Koeffizienten $a_0, \dots, a_5$ um einen Skalar abändern ohne die Quadrik zu ändern, d.h. eine Quadrik wird gegeben durch einen Punkt $(a_0 : a_1 : \dots : a_5) \in \mathbf{P}^5$. Wir können die Menge aller ebenen Quadriken also betrachten als eine projektiven Raum der Dimension 5. Sei nun
$$X = \{(a_0 : \dots : a_5) \in \mathbf{P}^5 : f_{(a_0,\dots,a_5)} \text{ ist reduzibel}\}.$$
Was kann man über X sagen? Eine Quadrik $f_{(a_0,\dots,a_5)}$ ist genau dann reduzibel, wenn es $b_0, b_1, b_2, c_0, c_1, c_2 \in \overline{K}$ gibt mit
$$\begin{aligned} f &= (b_0x_0 + b_1x_1 + b_2x_2)(c_0x_0 + c_1x_1 + c_2x_2) = \\ &= b_0c_0x_0^2 + (b_0c_1 + b_1c_0)x_0x_1 + (b_0c_2 + b_2c_0)x_0x_2 + b_1c_1x_1^2 + (b_1c_2 + b_2c_1)x_1x_2 + b_2c_2x_2^2, \end{aligned}$$
also
$$a_0 = b_0c_0, \quad a_1 = b_0c_1 + b_1c_0, \quad a_2 = b_0c_2 + b_2c_0, \quad a_3 = b_1c_1, \quad a_4 = b_1c_2 + b_2c_1, \quad a_5 = b_2c_2.$$
Definieren wir also $\phi : \mathbf{P}^1 \times \mathbf{P}^1 \to \mathbf{P}^5$ durch
$$((b_0 : b_1 : b_2), (c_0 : c_1 : c_2)) \mapsto (b_0c_0 : b_0c_1 + b_1c_0 : b_0c_2 + b_2c_0 : b_1c_1 : b_1c_2 + b_2c_1 : b_2c_2),$$
so ist ϕ ein Morphismus mit Bild X. Daher ist X abgeschlossen, d.h. X läßt sich durch Gleichungen beschreiben. Man findet
$$X = \{4a_0a_3a_5 + a_1a_2a_4 - a_0a_4^2 - a_1^2a_5 - a_2^2a_3 = 0\}.$$

Bevor wir weitermachen, geben wir noch zwei einfache Lemmats an:

LEMMA 2. *Jeder Morphismus ist stetig in der Zariski-Topologie.*

Beweis: Ein Morphismus $\phi : X \to Y$ wird lokal gegeben durch $\phi = (f_0 : \dots : f_n)$ mit homogenen Polynomen gleichen Grades f_i. Eine abgeschlossene Menge in Y wird gegeben durch homogene Gleichungen $F_1 = \dots = F_r = 0$. Das Urbild ist dann
$$F_1(f_0, \dots, f_n) = \dots = F_r(f_0, \dots, f_n) = 0,$$
also wieder abgeschlossen. ■

LEMMA 3. *Sei $\phi : X \to Y$ ein Morphismus und X irreduzibel. Dann ist auch $\phi(X)$ irreduzibel.*

Beweis: Sei $\phi(X) = Z_1 \cup Z_2$ mit (in $\phi(X)$) abgeschlossenen Mengen Z_1, Z_2. Dann ist $X = \phi^{-1}(Z_1) \cup \phi^{-1}(Z_2)$, also gilt wegen der Irreduzibilität von X für ein i: $X = \phi^{-1}(Z_i)$ und damit $\phi(X) = Z_i$. ■

Trivialerweise folgt damit:

FOLGERUNG 1. *Ist X eine projektive Varietät und $\phi : X \to \mathbf{P}^n$ ein Morphismus, so ist $\phi(X)$ eine projektive Varietät.*

Wir beweisen jetzt noch einen Satz, den wir schon zitiert haben.

SATZ 7. *Sei X eine projektive Varietät und $f \in \overline{K}(X)$ eine Funktion, die auf ganz X definiert ist. Dann ist $f \in \overline{K}$.*

Beweis: f liefert eine Funktion $X \to \mathbf{A}^1 \subseteq \mathbf{P}^1$, also einen Morphismus $f : X \to \mathbf{P}^1$. Das Bild ist abgeschlossen, $\neq \mathbf{P}^1$, besteht also aus endlich vielen Punkten, also aus genau einem Punkt $a \in \mathbf{P}^1$, $a \in \mathbf{A}^1$. Also ist f konstant. ■

Eine etwas allgemeinere Formulierung obiger Aussage ist folgende:

SATZ 8. *Sei $\phi : V \to W$ ein Morphismus zwischen projektiven Varietäten. Dann ist ϕ eine abgeschlossene Abbildung, d.h. abgeschlossene Mengen werden in abgeschlossene abgebildet.*

Beweis: O.E. $V \subseteq \mathbf{P}^m$ und $W \subseteq \mathbf{P}^n$. Sei $Z \subseteq V$ abgeschlossen. Dann gibt es eine Zerlegung $Z = Z_1 \cup \cdots \cup Z_r$, wo die Z_i abgeschlossen und irreduzibel sind. Also sind die $Z_i \subseteq \mathbf{P}^m$ projektive Varietäten. ϕ induziert natürlich auch Morphismen $\phi : Z_i \to \mathbf{P}^n$. Also ist $\phi(Z_i)$ abgeschlossen und damit auch $\phi(Z) = \phi(Z_1) \cup \cdots \cup \phi(Z_r)$. ■

DEFINITION 20. *Ein Morphismus $\phi : V \to W$ zwischen projektiven Varietäten heißt eine Einbettung, falls ϕ einen Isomorphismus zwischen V und (der projektiven Varietät) $\phi(V)$ liefert.*

Beispiel: Wir definieren

$$\phi : \mathbf{P}^1 \times \mathbf{P}^1 \to \mathbf{P}^3, \quad ((x_0 : x_1), (y_0, y_1)) \mapsto (x_0y_0 : x_0y_1 : x_1y_0 : x_1y_1).$$

ϕ ist ein Morphismus und $\phi(\mathbf{P}^1 \times \mathbf{P}^1) \subseteq Q = \{z_0z_3 = z_1z_2\}$. Wir wollen eine Umkehrabbildung finden. Dazu überlegen wir zunächst: Ist $z_0 = 1$, so o.E. $x_0 = y_0 = 1$ und $x_1 = z_2$, $y_1 = z_1$. Wegen

$$(z_0 : z_1) = (z_0z_3 : z_1z_3) = (z_1z_2 : z_1z_3) = (z_2 : z_3)$$

und

$$(z_0 : z_2) = (z_0z_3 : z_2z_3) = (z_1z_2 : z_2z_3) = (z_1 : z_3)$$

setzen wir an: $\psi : Q \to \mathbf{P}^1 \times \mathbf{P}^1$ mit

$$\psi = ((z_0 : z_2), (z_0 : z_1)) = ((z_0 : z_2), (z_2 : z_3)) = ((z_1 : z_3), (z_0 : z_1)) = ((z_1 : z_3), (z_2 : z_3)).$$

Offensichtlich ist auch ψ ein Morphismus und man rechnet schnell nach, daß $\phi\psi$ und $\psi\phi$ jeweils die Identität sind. Also ist $\mathbf{P}^1 \times \mathbf{P}^1$ isomorph zur Quadrik Q im $\mathbf{P}^3$.

Dieses Beispiel verallgemeinert sich wie folgt:

SATZ 9. *Definiert man $\phi : \mathbf{P}^m \times \mathbf{P}^n \to \mathbf{P}^{mn+m+n}$ durch*

$$((x_0 : \cdots : x_m), (y_0 : \cdots : y_n)) \mapsto (x_0y_0 : \cdots : x_0y_n : \cdots : x_my_0 : \cdots : x_my_n),$$

so ist ϕ eine Einbettung, die sogenannte Segre-Einbettung. Insbesondere ist $\mathbf{P}^m \times \mathbf{P}^n$ eine projektive Varietät.

Wir wollen nochmals rationale Abbildungen betrachten. Da rationale Abbildungen nicht überall definiert sein müssen, kann man nicht allgemein eine Komposition definieren.

DEFINITION 21. *Sei $\phi : V \to W$ eine rationale Abbildung mit maximaler Definitionsmenge U. Wir sagen, ϕ ist generisch surjektiv, falls $\phi(U)$ dicht in W liegt.*

Beispiel: Wir betrachten die rationale Abbildung $\phi : \mathbf{P}^2 \to \mathbf{P}^2$ mit

$$\phi = (\frac{1}{x_0} : \frac{1}{x_1} : \frac{1}{x_2}) = (x_1x_2 : x_0x_2 : x_0x_1).$$

ϕ ist eine sogenannte quadratische Transformation der Ebene. ϕ ist generisch surjektiv und $\phi \circ \phi = id$. Was passiert geometrisch? ϕ ist nicht definiert in den 3 Punkten $(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)$. Die Gerade $x_0 = 0$ wird auf $(1 : 0 : 0)$ zusammengezogen, $x_1 = 0$ auf $(0 : 1 : 0)$, $x_2 = 0$ auf $(0 : 0 : 1)$.

Der folgende Satz Identitätssatz für rationale Abbildungen wird oft benutzt.

SATZ 10. *Seien $\phi_1, \phi_2 : X \to Y$ zwei rationale Abbildungen zwischen projektiven Varietäten mit maximaler Definitionsmenge U_1 und U_2. Stimmen ϕ_1 und ϕ_2 auf einer offenen Teilmenge $U \neq \emptyset$ überein, so gilt schon $\phi_1 = \phi_2$.*

Beweisidee: $U_1 \cap U_2 \cap \{\phi_1 \neq \phi_2\}$ ist eine offene Menge, $U \subseteq U_1 \cap U_2 \cap \{\phi_1 = \phi_2\}$ ebenso. Wir wissen, daß je zwei offene nichtleere Mengen einen nichtleeren Durchschnitt besitzen. Wegen $U \neq \emptyset$, folgt also $U_1 \cap U_2 \cap \{\phi_1 \neq \phi_2\} = \emptyset$, d.h. ϕ_1 und ϕ_2 stimmen auf $U_1 \cap U_2$ überein. Dann kann man aber ϕ_1 auch auf $U_1 \cup U_2$ fortsetzen. Also folgt $U_1 = U_2$ und damit die Behauptung. ■

Man hätte diesen Satz auch mit folgenden Lemma beweisen können.

LEMMA 4. *Ist X eine projektive Varietät und $f, g \in \overline{K}$ zwei Funktionen, die auf einer offenen nichtleeren Menge U übereinstimmen, dann gilt schon $f = g$ (im Funktionenkörper).*

Beweis: Es genügt, $U \subseteq X \cap \mathbf{A}^n$ zu betrachten. Wir schreiben $f = \frac{f_1(x_1,\dots,x_n)}{f_2(x_1,\dots,x_n)}$ und $g = \frac{g_1(x_1,\dots,x_n)}{g_2(x_1,\dots,x_n)}$ als Quotient von Polynomen. Dann gilt auf U auch $f_1 g_2 - f_2 g_1 = 0$. Nun definiert $f_1 g_2 - f_2 g_1 \neq 0$ eine offene Menge in $X \cap \mathbf{A}^n$. Da je zwei offene nichtleere Mengen einen nichttrivialen Durchschnitt haben, muß $f_1 g_2 - f_2 g_1 \neq 0$ die leere Menge sein. Also gilt $f = g$ im Funktionenkörper. ■

DEFINITION 22. *Zwei projektive Varietäten heißen birational äquivalent über $\overline{K}$, falls es generisch surjektive rationale Abbildungen $\phi : V \to W$ und $\psi : W \to V$ gibt, so daß die rationalen Abbildungen $\phi\psi$ und $\psi\phi$ jeweils die Identität sind.*

Natürlich sind isomorphe projektive Varietäten auch birational äquivalent. Die birationale Äquivalenz ist aber i.a. eine gröbere Klassifizierung. Eine wesentliche Aufgabe der algebraischen Geometrie ist die Klassifizierung projektiver Varietäten bis auf birationale Äquivalenz.

Beispiel: Natürlich sind $\mathbf{A}^2$ und $\mathbf{A}^1 \times \mathbf{A}^1$ isomorph. Wie steht dies mit $\mathbf{P}^2$ und $\mathbf{P}^1 \times \mathbf{P}^1$? Wir definieren rationale Abbildungen

$$\phi : \mathbf{P}^1 \times \mathbf{P}^1 \to \mathbf{P}^2, \quad ((x_0 : x_1), (y_0 : y_1)) \mapsto (1 : \frac{x_1}{x_0} : \frac{y_1}{y_0}) = (x_0 y_0 : y_0 x_1 : x_0 y_1)$$

und

$$\psi : \mathbf{P}^2 \to \mathbf{P}^1 \times \mathbf{P}^1, \quad (z_0 : z_1 : z_2) \mapsto ((1 : \frac{z_1}{z_0}), (1 : \frac{z_2}{z_0})) = ((z_0 : z_1), (z_0 : z_2)).$$

Dann gilt $\psi\phi = id$ und $\phi\psi = id$, also sind $\mathbf{P}^1 \times \mathbf{P}^1$ und $\mathbf{P}^2$ birational äquivalent. Man kann zeigen, daß $\mathbf{P}^1 \times \mathbf{P}^1$ und $\mathbf{P}^2$ nicht isomorph sind: Auf $\mathbf{P}^1 \times \mathbf{P}^1$ gibt es Kurven, die sich nicht schneiden, z.B. $\{0\} \times \mathbf{P}^1$ und $\{1\} \times \mathbf{P}^1$, auf $\mathbf{P}^2$ schneiden sich dagegen je zwei Kurven in mindestens einem Punkt.

Beispiel: $X \subseteq \mathbf{P}^2$ werde definiert durch $y^2 = x^3$, d.h. $X = \{x_0 x_2^2 = x_1^3\}$. Dann haben wir gesehen, daß $\phi : X \to \mathbf{P}^1$ mit $\phi = (1 : \frac{y}{x})$ eine rationale Abbildung ist, die im Punkt $(1 : 0 : 0)$ nicht definiert ist. Sei $\psi : \mathbf{P}^1 \to X$ mit $\psi = (1 : t^2 : t^3)$. Man rechnet nach, daß ψ ein Morphismus ist. Außerdem gilt: $\phi\psi = id$, $\psi\phi = id$, d.h. X ist birational äquivalent zu $\mathbf{P}^1$. Allerdings ist X nicht isomorph zu $\mathbf{P}^1$. (X hat eine Singularität.)

Die Beispiele deuten schon einen Sachverhalt an, den wir ohne Beweis angeben:

SATZ 11. *Seien X und Y birational äquivalente projektive Varietäten. Dann gibt es nichtleere offene Teilmengen $U_X \subseteq X$, $U_Y \subseteq Y$, die isomorph sind.*

Wir stellen nun noch eine Verbindung zur Algebra her: Seien $X \subseteq \mathbf{P}^m$ und $Y \subseteq \mathbf{P}^n$ projektive Varietäten.

- Haben wir auf $\mathbf{P}^m$ die Koordinaten x_i, auf $\mathbf{P}^n$ die Koordinaten y_j, so können wir uns die Funktionenkörper denken als $K(X) = K(x_1, \dots, x_m)$ und $K(Y) = K(y_1, \dots, y_n)$ mit Relationen zwischen den x_i's und den y_j's.
- Sei $\phi : X \to Y$ eine generisch surjektive (rationale) Abbildung. Dann liefert

  $$\phi^* : K(Y) \to K(X), \quad f \mapsto f \circ \phi$$

  einen Körperhomomorphismus, der K festläßt. Er ist dadurch festgelegt, daß man die $\phi^*(y_j)$'s kennt. ϕ^* ist (als Körperhomomorphismus) injektiv.

- Davon gilt nun auch die Umkehrung: Sei
$$\alpha : K(Y) \to K(X)$$
ein Körperhomomorphismus, der K in sich überführt. Sei $\alpha(y_i) = f_i(x_1, \dots, x_n)$ mit $f_i \in K(X)$. Dann gibt es eine rationale Abbildung $\phi : X \to Y$ mit
$$\phi = (1 : f_1 : \dots : f_n).$$
- Wieso ist ϕ generisch surjektiv? Sei F ein Polynom mit $F(f_1, \dots, f_n) = 0$, also $\alpha(F(y_1, \dots, y_n)) = 0$ und damit $F(y_1, \dots, y_n) = 0$. Dies liefert $F \in I(Y)$, also eine Relation, die trivialerweise erfüllt sein muß. Daher ist ϕ generisch surjektiv.
- Was ist ϕ^*? Dazu bestimmen wir die Urbilder der Koordinatenfunktionen y_j. Wegen $\phi = (1 : f_1 : \dots : f_n)$ ist $\phi^*(y_j) = f_j$. Also $\phi^*(y_j) = \alpha(y_j)$. Da die y_j's den Funktionenkörper erzeugen, folgt $\phi^* = \alpha$.

Damit haben wir folgenden Satz bewiesen:

SATZ 12. *Für projektive Varietäten X und Y gibt es eine Bijektion*
$$\{\phi : X \to Y \text{ generisch surjektiv }\} \simeq \{\alpha : \overline{K}(Y) \to \overline{K}(X) \text{ Körperhomomorphismus mit } \alpha|_{\overline{K}} = id|_{\overline{K}}\}$$
vermöge $\alpha = \phi^*$.

Beispiel: Sei C eine irreduzible projektive Kurve. Jede rationale Abbildung $\phi : C \to \mathbf{P}^1$ ist gegeben durch $\phi = (f_0 : f_1)$ mit $f_0, f_1 \in \overline{K}(C)$. O.E. ist $f_0 \neq 0$. Mit $f = \frac{f_1}{f_0}$ kann man dann auch $\phi = (1 : f)$ schreiben. Es gibt zwei Möglichkeiten:

- ϕ ist konstant, d.h. $f \in \overline{K}$.
- ϕ ist nicht konstant, d.h. $f \in \overline{K}(C) \setminus \overline{K}$. Dann ist ϕ generisch surjektiv. Hat man auf $\mathbf{P}^1$ die Koordinaten $(1 : t)$, so ist ϕ^* gegeben durch
$$\overline{K}(t) \to \overline{K}(C), \quad t \mapsto f.$$
Umgekehrt schaut hat natürlich auch jeder Körperhomomorphismus $\overline{K}(t) \to \overline{K}(C)$, der $\overline{K}$ festläßt, so aus.

Beispiel: Sei $F_n \subseteq \mathbf{P}^2$ gegeben durch $x^n + y^n = 1$. Der Funktionenkörper von F_n ist
$$\overline{K}(F_n) = \overline{K}(x, y) \text{ mit } x^n + y^n = 1.$$
Auf $\mathbf{P}^1$ wählen wir Koordinaten $(1 : t)$. Dann ist der Funktionenkörper von $\mathbf{P}^1$ einfach $\overline{K}(t)$. Wir suchen eine nichtkonstante (also generisch surjektive) rationale Abbildung $\phi : \mathbf{P}^1 \to F_n$.
Algebraische Interpretation: Wir suchen einen $\overline{K}$ festlassenden Körperhomomorphismus
$$\alpha : \overline{K}(x, y) \to \overline{K}(t) \text{ (mit)} x^n + y^n = 1.$$
$\alpha(x)$ und $\alpha(y)$ sind dann rationale Funktionen in t mit $(\alpha(x))^n + (\alpha(y))^n = 1$. Da $\overline{K}$ fest bleibt, sind $\alpha(x)$ und $\alpha(y)$ nicht konstant. Wir setzen an $\alpha(x) = \frac{f}{h}, \alpha(y) = \frac{g}{h}$ und erhalten dann die Bedingung $f^n + g^n = h^n$, wobei wir also f, g, h als paarweise teilerfremde Polynome in t annehmen können, die nicht alle konstant sind.
Geometrische Interpretation: Wir suchen Polynome f, g, h in t mit $\phi = (h : f : g)$. Da das Bild von ϕ in C liegen soll, muß gelten $f^n + g^n = h^n$. Wir können annehmen, daß f, g, h paarweise teilerfremd sind. Da ϕ nicht konstant sein soll, sollen f, g, h nicht alle konstant sein.
Behauptung: Für $n \geq 3$ und $char(K) = 0$ gibt es keine solchen Polynome.
Beweis: Wir nehmen an, wir haben eine nichttriviale Relation $f^n + g^n = h^n$. Insbesondere sind alle $f, g, h \neq 0$. Differenzieren liefert $nf^{n-1} \cdot f' + ng^{n-1} \cdot g' = nh^{n-1} \cdot h'$. Wir schreiben dies in Matrizenform:
$$\begin{pmatrix} f & g & h \\ f' & g' & h' \end{pmatrix} \begin{pmatrix} f^{n-1} \\ g^{n-1} \\ -h^{n-1} \end{pmatrix} = 0.$$
Als Grundkörper haben wir jetzt $\overline{K}(t)$. Sei
$$M = \begin{pmatrix} f & g & h \\ f' & g' & h' \end{pmatrix}.$$

Das Gleichungssytem $M \cdot X = 0$ hat immer die Lösung

$$\left(\begin{vmatrix} g & h \\ g' & h' \end{vmatrix}, \begin{vmatrix} h & f \\ h' & f' \end{vmatrix}, \begin{vmatrix} f & g \\ f' & g' \end{vmatrix} \right).$$

1. Fall: Der Rang von M ist 1. Dann müssen obige Unterdeterminanten 0 sein. Also $fg' = f'g$ etc. Da f und g teilerfremd sind, folgt $f|f'$, was aus Gradgründen sofort $f' = 0$ impliziert, also $f \in \overline{K}$. Genauso folgt $f, g, h \in \overline{K}$, ein Widerspruch.
2. Fall: M hat Rang 2. Dann hat das Gleichungssystem $M \cdot X = 0$ einen 1-dimensionalen Lösungsraum, also gibt es teilerfremde Polynome $r(t), s(t)$ mit

$$f^{n-1} = \frac{r}{s} \begin{vmatrix} g & h \\ g' & h' \end{vmatrix}, \; g^{n-1} = \frac{r}{s} \begin{vmatrix} h & f \\ h' & f' \end{vmatrix}, \; -h^{n-1} = \frac{r}{s} \begin{vmatrix} f & g \\ f' & g' \end{vmatrix}.$$

Bringt man s auf die andere Seite, so sieht man sofort $r|f^{n-1}, g^{n-1}, h^{n-1}$, und da f, g, h teilerfremd sind: $r \in \overline{K}$, also o.E. $r = 1$. Jetzt folgt

$$f^{n-1}|(gh' - g'h), \; g^{n-1}|(hf' - h'f), \; h^{n-1}|(fg' - f'g).$$

Wir wollen jetzt die Grade vergleichen. Setzt man a, b, c für den Grad von f, g, h, so folgt

$$(n-1)a \leq b + c - 1, \quad (n-1)b \leq c + a - 1, \quad (n-1)c \leq a + b - 1,$$

oder auch

$$na, nb, nc \leq a + b + c - 1.$$

Setzt man $d = \max(a, b, c)$, so ist $d \geq 1$ und $nd \leq 3d - 1$, also $n \leq 2$, ein Widerspruch zu unserer Annahme. Damit ist die Behauptung bewiesen. ∎
Bemerkung: Für $n = 1$ kann man $f = t, g = 1 - t, h = 1$ wählen, für $n = 2$:

$$f = 2t, \quad g = t^2 - 1, \quad h = t^2 + 1.$$

Damit folgt sofort:

SATZ 13. *Zwei projektive Varietäten V und W sind genau dann birational äquivalent über $\overline{K}$, falls die Funktionenkörper $\overline{K}(V)$ und $\overline{K}(W)$ über $\overline{K}$ isomorph sind.*

FOLGERUNG 2. *Jede projektive Varietät V der Dimension d ist birational äquivalent zu einer Hyperfläche $f = 0$ im $\mathbf{P}^{d+1}$. Ist V über K definiert, so kann auch $f = 0$ und die birationale Äquivalenz über K definiert werden.*

Beweis: Der Funktionenkörper $K(V)$ hat Transzendenzgrad d über K. Dann gibt es algebraisch unabhängige Elemente $t_1, \ldots, t_f \in K(V)$, so daß $K(V)$ eine endliche (algebraische) Erweiterung von $K(t_1, \ldots, t_d)$ ist. Man kann es so einrichten, daß $K(V)$ über $K(t_1, \ldots, t_d)$ separabel ist. Also gibt es ein $u \in K(V)$ mit $K(V) = K(t_1, \ldots, t_d, u)$. Außerdem besteht eine algebraische Relation $f(t_1, \ldots, t_d, u) = 0$ (Polynom mit Koeffizienten aus K), wobei das Polynom f irreduzibel gewählt werden kann. Der Funktionenkörper der Hyperfläche

$$f(x_1, \ldots, x_d, x_{d+1}) = 0$$

im $\mathbf{P}^{d+1}$ ist $Quot(K[x_1, \ldots, x_{d+1}]/(f))$, also $K(V)$. Nach unserem Satz ist also V birational äquivalent zu der Hyperfläche $f = 0$. ∎

FOLGERUNG 3. *Jede irreduzible projektive Kurve ist birational äquivalent zu einer ebenen Kurve $\{f(x_0, x_1, x_2) = 0\} \subseteq \mathbf{P}^2$.*

KAPITEL 3

Algebraische Kurven

Unter einer Kurve verstehen wir im folgenden eine irreduzible projektive Kurve C, die wir uns als $C \subseteq \mathbf{P}^n$ denken.

Sei also C eine Kurve. Wir haben dann den Funktionenkörper $\overline{K}(C)$ definiert. Für $P \in C$ haben wir den lokalen Ring von C in P definiert:

$$\overline{K}[C]_P = \{f \in \overline{K}(C) : f \text{ ist definiert in } P\}.$$

Darin gibt es die Einheiten

$$\overline{K}[C]_P^\times = \{f \in \mathcal{O}_P : f(P) \neq 0\} = \{\frac{g}{h} \in \overline{K}(C) : g, h \text{ Polynome mit } g(P), h(P) \neq 0\}$$

und das maximale Ideal

$$\mathfrak{m}_P = \{f \in \mathcal{O}_P : f(P) = 0\}.$$

Wir betrachten zunächst ein Beispiel:

Beispiel: Wir betrachten $\mathbf{P}^1$ und den Punkt $(1:1) \simeq 1$. Der Funktionenkörper ist $K(x)$. Jedes $f \in K(x), f \neq 0$ hat eine eindeutige Darstellung $f = u(x) \cdot (x-1)^n$ mit $n \in \mathbf{Z}$, wo u in 1 definiert ist und $u(1) \neq 0$. n ist dann die Null- bzw. Polstellenordnung von f im Punkt 1.

Dieses Beispiel ist typisch für nichtsinguläre Punkte auf Kurven, wie folgender wichtige Satz besagt:

Satz 14. *Sei C eine Kurve und P ein nichtsingulärer Punkt auf C. Dann ist der lokale Ring von C in P ein diskreter Bewertungsring, d.h. es gibt eine Funktion t, die in P definiert ist, so daß sich jedes Element $f \neq 0$ des lokalen Rings eindeutig schreiben läßt als $f = ut^n$ mit einer Einheit u und $n \geq 0$. t heißt Ortsuniformisierende in P. Jedes Element $f \neq 0$ aus $\overline{K}(C)$ hat eine eindeutige Darstellung*

$$f = ut^n \text{ mit } u(P) \neq 0 \text{ und } n \in \mathbf{Z}.$$

Der Exponent n wird auch mit $v_P(f)$ bezeichnet. Ist $v_P(f) > 0$, so sagt man, f hat in P eine Nullstelle, ist $v_P(f) < 0$, so sagt man, f hat in P eine Polstelle.

Beweisidee:

- Der Einfachkeit halber beschränken wir uns auf den Fall $C \subseteq \mathbf{P}^2$. Nach Koordinatenwechsel können wir $P = (0,0) \in \mathbf{A}^2 \subseteq \mathbf{P}^2$ und $C \cap \mathbf{A}^2 = \{F(x,y) = 0\}$ annehmen. Wir betrachten die Taylorreihenentwicklung von F in $P = (0,0)$:

  $$F = ax + by + \text{ Terme mit Monomen vom Grad } \geq 2.$$

  Da C in P nichtsingulär sein soll, ist a oder $b \neq 0$. Nach einem weiteren Koordinatenwechsel können wir o.E. $b \neq 0$, auch $b = 1$ annehmen und dann

  $$F = y + ax + \text{ Terme mit Monomen vom Grad } \geq 2$$

  annehmen.
- Wir klammern jetzt y überall aus und erhalten eine Darstellung

  $$F = y(1 + a(x,y)) - b(x)x$$

  mit Polynomen a und b und $a(0,0) = 0$. Im Funktionenkörper gilt also

  $$y = \frac{b(x)x}{1 + a(x,y)}.$$

- Nun ist $\overline{K}[C] = \overline{K}[x,y]/(F)$, das maximale Ideal des lokalen Rings wird also von x und y erzeugt. Mit unserer Relation folgt: $\mathfrak{m}_P = (x)$.
- Sei nun $f \in \overline{K}[C]_P$. Ist $f(P) \neq 0$, so ist f Einheit und wir sind fertig. Ist $f(P) = 0$, so ist $f \in \mathfrak{m}_P$, also gibt es $f_1 \in \overline{K}[C]_P$ mit $f = f_1 \cdot x$. Nun kann man das gleiche Spiel mit f_1 machen, u.s.w. Man erhält $f_i = f_{i+1} \cdot x$, solange $f_i(P) = 0$ ist. Damit gilt
$$f = f_1 x = f_2 x^2 = \cdots = f_i x^i.$$
- Warum muß dieser Prozeß aufhören? Es ist $f_i = f_{i+1}x$, also $(f_i) \subset (f_{i+1})$ und somit
$$(f) \subset (f_1) \subset (f_2) \subset \ldots.$$
Der Hilbertsche Basissatz besagt nun, daß es keine unendlich echt aufsteigende Idealkette geben kann. Also bricht der Prozeß ab.
- Jedes Element hat also die Form $f = ux^n$ mit $u(P) \neq 0$ und $n \geq 0$.
- Zur Eindeutigkeit: $ux^m = vx^n$ mit Einheiten u, v und $m \geq n \geq 0$. Dann ist $ux^{m-n} = v$ Einheit, also $m = n$ und $u = v$.
- Jedes Element $f \neq 0$ im Funktionenkörper läßt sich als Quotient von Polynomen, insbesondere als Quotient von Elementen aus $\overline{K}[C]_P$ darstellen. Daraus folgt die letzte Behauptung. ■

Bemerkungen:

1. Ist $C \cap \mathbf{A}^2 = \{F(x,y) = 0\}$ und $P = (a,b)$ ein nichtsingulärer Punkt auf C, so ist
$$\frac{\partial F}{\partial x}(P)(x-a) + \frac{\partial F}{\partial y}(P)(y-b) = 0$$
die Tangente. Als Uniformisierende kann man irgendeine Linearform $t = A(x-a) + B(y-a)$ wählen, die nicht die Tangente definiert.
2. Ist $\frac{\partial F}{\partial x}(P) \neq 0$, so ist $y - b$ uniformisierend, ist $\frac{\partial F}{\partial y}(P) \neq 0$, so ist $x - a$ uniformisierend.
3. Ist $C \subseteq \mathbf{P}^n$ und $P \in C \cap \mathbf{A}^n$, so kann man als Uniformisierende jede Hyperebene t durch P wählen, die nicht die Tangente von C in P enthält.

Bemerkung: Sei P ein nichtsingulärer Punkt auf der Kurve C. Die Funktion v_P kann man dann als Funktion
$$v_P : \overline{K}(C) \to \mathbf{Z} \cup \{\infty\}$$
betrachten, wenn man noch $v_P(0) = \infty$ setzt. Man hat die folgenden Eigenschaften:

- $v_P(fg) = v_P(f) + v_P(g)$,
- $v_P(f+g) \geq \min(v_P(f), v_P(g))$,
- ist $v_P(f) \neq v_P(g)$, so gilt $v_P(f+g) = \min(v_P(f), v_P(g))$,
- v_P ist surjektiv.

Beispiel: Sei $C \subseteq \mathbf{P}^2$ definiert durch $y^2 = x^3 - 1$, d.h. $C = \{x_0 x_2^2 = x_1^3 - x_0^3\}$.
Im Endlichen: Sei $(a,b) \in C$. Die Tangente ist $-3a^2(x-a) + 2b(y-b) = 0$. Ist $b \neq 0$, so ist $x - a$ uniformisierend, ist $b = 0$, so ist y uniformisierend.
Im Unendlichen: Es gibt nur den Punkt $(0:0:1)$. Wir erhalten affine Koordinaten durch $(u:v:1)$. Die Gleichung lautet hier $u = v^3 - u^3$. Im Punkt $P = (0:0:1)$ ist $u = 0$ Tangente, also v uniformisierend. Mit
$$(1:x:y) = (u:v:1) = (1:\frac{v}{u}:\frac{1}{u})$$
erhält man $x = \frac{v}{u}$ und $y = \frac{1}{u}$.
Wir wollen jetzt die Null- und Polstellen der Funktion $f = y$ bestimmen.
Im Endlichen: Hier hat y keine Polstelle. Es gibt 3 Nullstellen: $P_1 = (1,0), P_2 = (\zeta,0), P_3 = (\zeta^2,0)$, wo $\zeta = \frac{-1+\sqrt{-3}}{2}$ eine primitive dritte Einheitswurzel ist. In allen 3 Punkten ist y uniformisierend, also $v_{P_i}(y) = 1$, d.h. in allen 3 Punkten hat y eine einfache Nullstelle.
Im Unendlichen: Ist ist $\frac{1}{y} = u$. Wir haben $u = v^3 - u^3$, v ist uniformisierend. Auch u hat eine Nullstelle. Wegen $u(1+u^2) = v^3$ gilt $u = \frac{1}{1+u^2}v^3$, also folgt sofort $v_P(u) = 3$ und daher $v_P(y) = -3$.

Beispiel: In $\mathbf{P}^1$ haben wir den offenen endlichen Teil $\mathbf{A}^1 = \{(1:t) : t \in \mathbf{A}^1\}$ mit Koordinate t und den unendlich fernen Punkt $\infty = (0:1)$. Eine offene affine Umgebung von ∞ ist $\{(u:1) : u \in \mathbf{A}^1\}$ mit

Koordinate t. Es gilt $u = \frac{1}{t}$.
In $a \in \mathbf{A}^1$ ist $t - a$ uniformisierend, in ∞ die Funktion $u = \frac{1}{t}$.
Jedes $f \in \overline{K}(t), f \neq 0$ hat eine eindeutige Zerlegung

$$f = c \prod_{i=1}^{n} (t - a_i)^{e_i},$$

wobei $a_1, \ldots, a_n, c \in \overline{K}$ und $e_i \in \mathbf{Z}$ sind. Natürlich kann man annehmen, daß alle a_i verschieden sind. Dann gilt

$$v_{a_i}(f) = e_i.$$

Was ist v_∞? Wir schreiben

$$f = \frac{a_0 t^m + \cdots + a_m}{b_0 t^n + \cdots + b_n}$$

mit $a_0, b_0 \neq 0$. Dann gilt

$$f = u^{n-m} \cdot \frac{a_0 + a_1 u + \cdots + a_m}{b_0 + b_1 u + \cdots + b_n u^n}.$$

Der Bruch ist in ∞ definiert und hat den Wert $\frac{a_0}{b_0}$. Also gilt $v_\infty(f) = n - m$. Dies paßt auch mit der natürlichen Vorstellung zusammen, was passiert, wenn $\lim_{t \to \infty} f(t)$ gebildet wird — was aber bei uns nicht definiert wird.

FOLGERUNG 4. *Sei C eine Kurve, Y eine projektive Varietät $\phi : C \to Y$ eine rationale Abbildung. Ist $P \in C$ ein nichtsingulärer Punkt von C, so ist ϕ in P definiert.*

Beweis: Sei $\phi = (f_0 : \cdots : f_n)$ mit $f_i \in \overline{K}(C)$. Sei t uniformisierend in P. Wir können o.E. $f_i \neq 0$ annehmen, sonst lassen wir die entsprechende Koordinate weg. Dann ist $f_i = u_i \cdot t^{e_i}$, wo u_i Einheit in P ist. Sei o.E. $e_0 = \min(e_0, \ldots, e_n)$. Dann gilt

$$\phi = (u_0 : u_1 t^{e_1 - e_0} : \cdots : u_n t^{e_n - e_0})$$

und man sieht an dieser Darstellung, daß ϕ in P definiert ist. ■

Damit folgt unmittelbar:

FOLGERUNG 5. *Ist C eine nichtsinguläre Kurve, Y eine projektive Varietät und $\phi : C \to Y$ eine rationale Abbildung, so ist ϕ schon ein Morphismus.*

FOLGERUNG 6. *Zwei birational äquivalente Kurven sind schon isomorph.*

Was bedeutet das? In einer Äquivalenzklasse birational äquivalenter Kurven gibt es bis auf Isomorphie höchstens eine nichtsinguläre Kurve. Es stellt sich dann sofort die Frage: Ist jede Kurve birational äquivalent zu einer nichtsingulären Kurve? Wie findet man eine solche? Wir wissen bereits, daß jede Kurve zu einer ebenen Kurve birational äquivalent ist. Wir werden jetzt Singularitäten ebener Kurven durch Aufblasen auflösen.

Vorbemerkung: Da Singularitäten ein lokales Phänomen sind, werden wir uns im folgenden auf die zweidimensionale affine Darstellung beschränken.

Aufblasen von $\mathbf{A}^2$ in $(0,0)$:

1. Sei
$$X = \{(x, y), (u : v)) \in \mathbf{A}^2 \times \mathbf{P}^1 : xv = yu\}$$
und $\pi : X \to \mathbf{A}^2$ die Projektion auf die erste Komponente. Man nennt π die Aufblasung von $\mathbf{A}^2$ in $P = (0,0)$.
2. Wir betrachten einen Punkt $((x, y), (u : v)) \in X$:
   - Fall $x \neq 0$: Dann ist $v = \frac{y}{x} u$ und
   $$((x, y), (u : v)) = ((x, y), (u : \frac{y}{x} u)) = ((x, y), (x : y)).$$
   - Fall $y \neq 0$: Dann ist $u = \frac{x}{y} v$ und
   $$((x, y), (u : v)) = ((x, y), (\frac{x}{y} v : v)) = ((x, y), (x : y)).$$

- Fall $x = y = 0$: Dann hat man keine Bedingung:
$$((0,0),(u:v)).$$

Also gilt
$$\pi^{-1}((x,y)) = \{((x,y),(x:y))\} \text{ falls } (x,y) \neq (0,0),$$
$$\pi^{-1}((0,0)) = \{((0,0),(u:v)) : (u:v) \in \mathbf{P}^1\}.$$
Definiert man jetzt $E = \{((0,0),(u:v)) \in X : (u:v) \in \mathbf{P}^1\}$, so ist offensichtlich
$$E = \pi^{-1}((0,0)) \simeq \mathbf{P}^1.$$
Man nennt E den exzeptionellen Divisor oder die exzeptionelle Faser.

3. Definiert man weiter $\phi : \mathbf{A}^2 \to X$ durch $(x,y) \mapsto ((x,y),(x:y))$, so ist ϕ definiert auf $\mathbf{A}^2 \setminus \{(0,0)\}$ und induziert einen Isomorphismus
$$X \setminus E \simeq \mathbf{A}^2 \setminus \{(0,0)\}.$$
Was ist also passiert? Man ersetzt in $\mathbf{A}^2$ den Punkt $(0,0)$ durch eine projektive Gerade, man *bläst auf.*
4. Wie rechnet man mit der Aufblasung? Wir betrachten die offene Überdeckung $X = \{u \neq 0\} \cup \{v \neq 0\}$:
   - Ist $u \neq 0$, so o.E. $u = 1$ und
   $$X \cap \{u \neq 0\} = \{((x,y),(1:v)) : xv = y\} = \{((x,xv),(1:v))\} \simeq \{(x,v) \in \mathbf{A}^2\} \simeq \mathbf{A}^2.$$
   In diesem affinen Teil bilden also x und v affine Koordinaten, E ist hier gegeben durch die einzige Gleichung $x = 0$.
   - Ist $v \neq 0$, so o.E. $v = 1$ und
   $$X \cap \{v \neq 0\} = \{((x,y),(u:1)) : x = yu\} = \{((yu,y),(u:1))\} \simeq \{(y,u) \in \mathbf{A}^2\} \simeq \mathbf{A}^2.$$
   In diesem affinen Teil bilden also y und u affine Koordinaten, E ist hier gegeben durch die einzige Gleichung $y = 0$.

   Wir können also Phänomene in den affinen Teilen $\{u \neq 0\}$ und $\{v \neq 0\}$ studieren. Oft kommt man mit einem Teil aus, denn
   $$\{u = 0\} = \{((0,y),(0:1))\} \text{ und } \{v = 0\} = \{((x,0),(1:0))\}.$$
5. Ist $C \subseteq \mathbf{A}^2$ eine Kurve, so enthält $\pi^{-1}(C)$ natürlich immer E, falls $(0,0) \in C$ ist. Daher definiert man das eigentliche Urbild von C als
$$\tilde{C} = \overline{\pi^{-1}(C \setminus \{(0,0)\})},$$
wo Überstreichen den Zariski-Abschluß bedeutet. Klar ist:
$$\tilde{C} \setminus E \simeq C \setminus \{(0,0\},$$
d.h. C und $\tilde{C}$ sind birational äquivalent. C und $\tilde{C}$ unterscheiden sich also nur in den Punkten von $\tilde{C} \cap E$. D.h. wenn man wissen will, wie Aufblasen C verändert, muß man nur die endlich vielen Punkte auf $\tilde{C} \cap E$ betrachten.

Beispiele:

1. Was passiert mit Geraden durch $(0,0)$? Betrachte $y = cx$. Dann ist das eigentliche Urbild $\{((x,cx),(1:c)) : x \in \overline{K}\}$, der Schnitt mit der exzeptionellen Faser E ist also $((0,0),(1:c))$, entspricht also genau der Steigung der Geraden. Verschiedene Geraden durch $(0,0)$ werden also beim Aufblasen auseinandergezogen.
2. Sei $C = \{y^2 = x^3\}$. Wir berechnen das eigentliche Urbild durch Betrachtung der affinen Überdeckung:
$\{u \neq 0\}$: Wir haben die affinen Koordinaten x, v mit $y = xv$. Einsetzen liefert $x^2v^2 = x^3$. Wir können durch x^2 dividieren, da wir zunächst die Situation außerhalb von E, d.h. von $x = 0$ studieren. Also folgt $x = v^2$. Damit ist $\tilde{C} \cap \{n \neq 0\} = \{x = v^2\}$, also nichtsingulär. $E \cap \tilde{C} \cap \{u \neq 0\} = \{((0,0),(1:0))\}$.
$\{v \neq 0\}$: Wir haben die affinen Koordinaten y, u mit $x = yu$. Einsetzen liefert $y^2 = y^3u^3$. Wieder können wir durch y^2 dividieren, da wir zunächst alles außerhalb von E, d.h. von $y = 0$ betrachten,

und erhalten: $1 = yu^3$. Damit gilt $\tilde{C} \cap \{v \neq 0\} = \{1 = yu^3\}$. Dies ist aber nicht interessant, da $\tilde{C} \cap E \cap \{v \neq 0\} = \emptyset$ ist.
Ergebnis: $\tilde{C}$ ist nichtsingulär und $E \cap \tilde{C} = \{((0,0),(1:0))\}$. Wir haben also C durch Aufblasen desingularisiert.

3. Sei $C = \{y^2 = x^2 + x^3\}$. Wir berechnen wieder das eigentliche Urbild durch Betrachtung der affinen Überdeckung:
$\{u \neq 0\}$: Wir haben die affinen Koordinaten x, v mit $y = xv$. Einsetzen liefert $x^2v^2 = x^2 + x^3$. Wir können durch x^2 dividieren, da wir zunächst die Situation außerhalb von E, d.h. von $x = 0$ studieren. Also folgt $v^2 = 1 + x$. Damit ist $\tilde{C} \cap \{n \neq 0\} = \{1 + x = v^2\}$, also nichtsingulär. $E \cap \tilde{C} \cap \{u \neq 0\} = \{((0,0),(1:1)),((0,0),(1:-1))\}$.
$\{v \neq 0\}$: Wir haben die affinen Koordinaten y, u mit $x = yu$. Einsetzen liefert $y^2 = y^2u^2 + y^3u^3$. Wieder können wir durch y^2 dividieren, da wir zunächst alles außerhalb von E, d.h. von $y = 0$ betrachten, und erhalten: $1 = u^2 + yu^3$. Damit gilt $\tilde{C} \cap \{v \neq 0\} = \{1 = u^2 + yu^3\}$, also
$$\tilde{C} \cap E \cap \{v \neq 0\} = \{((0,0),(1:1)),((0,0),(-1:1))\}.$$
Dies kennen wir bereits.
Ergebnis: $\tilde{C}$ ist nichtsingulär und $E \cap \tilde{C} = \{((0,0),(1:1)),((0,0),(1:-1))\}$. Wir haben also C durch Aufblasen desingularisiert.

Aufgabe: Löse die Singularitäten folgender ebener Kurven durch Aufblasen auf.

1. $x^2 = x^4 + y^4$
2. $xy = x^6 + y^6$
3. $x^3 = y^2 + x^4 + y^4$
4. $x^2y + xy^2 = x^4 + y^4$

Sei C eine ebene Kurve. Wie löst man die Singularitäten von C auf? Sei C_0 die Aufblasung von C in einem singulären Punkt. Dann ist $\pi_0 : C_0 \to C$ ein birationaler Morphismus. Ist C_0 noch singulär, so blase man einen singulären Punkt von C_0 auf. Man kann dies lokal, also affin machen. Man erhält $\pi_1 : C_1 \to C_0$, etc.
$$\cdots \to C_n \xrightarrow{\pi_n} C_{n-1} \xrightarrow{\pi_{n-1}} C_{n-2} \to \cdots \to C_1 \xrightarrow{\pi_1} C_0 \xrightarrow{\pi_0} C,$$
wobei die π_i birationale Morphismen sind. Die entscheidende Tatsache ist nun, daß man durch diesen Prozeß irgendwann bei einer nichtsingulären Kurve ankommt. (Ohne Beweis) Durch Aufblasen kann man also eine ebene Kurve desingularisieren. Damit erhält man schließlich:

SATZ 15. *Zu jeder irreduziblen projektiven Kurve C gibt es eine nichtsinguläre irreduzible projektive Kurve $\hat{C}$ und einen birationalen Morphismus $\pi : \hat{C} \to C$. Die Kurve $\hat{C}$ ist bis auf Isomorphie eindeutig bestimmt. Man sagt, $\hat{C}$ ist ein nichtsinguläres Modell von C.*

Bemerkung: Wir haben den Aufblasprozeß bisher nur affin 2-dimensional betrachtet. Man kann man auch allgemein einen Punkt im $\mathbf{P}^n$ aufblasen: Man nennt
$$X = \{((x_0 : x_1 : \cdots : x_n),(y_1 : \cdots : y_n)) \in \mathbf{P}^n \times \mathbf{P}^{n-1} : x_iy_j = x_jy_i \text{ für } i,j = 1,\ldots,n\}$$
zusammen mit der Projektion $\pi : X \to \mathbf{P}^n$ die Aufblasung von $\mathbf{P}^n$ im Punkt $(1:0:\cdots:0)$.

Wir wollen nochmals Morphismen zwischen glatten projektiven Kurven betrachten.

Beispiel: Sei $C \subseteq \mathbf{P}^2$ definiert durch $y^2 = x^3 - 1$ und $\phi : C \to \mathbf{P}^1$ durch $\phi = (1:y)$. Für $c \in \overline{K}$ gilt
$$\phi^{-1}((1:c)) = \{(1:x:c) \in C : x^3 = c^2 + 1\}.$$
Für $c \neq \pm i$ gibt es also genau 3 Urbilder von c. Außerdem gilt:
$$[\overline{K}(C) : \overline{K}(y)] = [\overline{K}(x,y) : \overline{K}(y)] = 3.$$
Dies ist nun ein ganz allgemeines Phänomen.

Sei $\phi : C_1 \to C_2$ ein Morphismus zwischen glatten projektiven Kurven. Wir wissen: ist ϕ nicht konstant, so ist ϕ surjektiv. Außerdem ist dann $\overline{K}(C_1)$ eine endliche algebraische Körpererweiterung von $\phi^*\overline{K}(C_2)$.

DEFINITION 23. *Sei $\phi : C_1 \to C_2$ ein nichtkonstanter Morphismus zwischen glatten projektiven Kurven. Dann heißt*

$$\deg \phi = [\overline{K}(C_1) : \phi^* \overline{K}(C_2)]$$

der Grad von ϕ. Man sagt, ϕ ist separabel, wenn die Körpererweiterung $\overline{K}(C_1)|\phi^*\overline{K}(C_2)$ separabel ist.

Um die Urbilder $\phi^{-1}(P)$ eines Punktes P richtig zu zählen, brauchen wir noch folgende Definition:

DEFINITION 24. *Sei $\phi : C_1 \to C_2$ ein nichtkonstanter Morphismus glatter projektiver Kurven und $P \in C_1$. Ist $t_{\phi(P)}$ eine Uniformisierende im Punkt $\phi(P)$, so heißt*

$$e_\phi(P) = v_P(\phi^* t_{\phi(P)})$$

der Verzweigungsindex von ϕ im Punkt P. (Wegen $(\phi^* t_{\phi(P)})(P) = t_{\phi(P)}(\phi(P)) = 0$ gilt immer $e_\phi(P) \geq 1$.) ϕ heißt verzweigt in P, falls $e_\phi(P) \geq 2$ gilt. ϕ heißt unverzweigt, falls $e_\phi(P) = 1$ für alle $p \in C_1$ gilt.

$e_\phi(P)$ zählt also, *wie oft* der Punkt P unter ϕ auf den Punkt $\phi(P)$ abgebildet wird. Dies wird noch deutlicher durch folgendes

Beispiel: Sei C eine glatte projektive Kurve und $f \in \overline{K}(C), f \notin \overline{K}$. Wir betrachten den Morphismus $\phi : C \to \mathbf{P}^1$ mit $\phi = (1 : f)$ und einen Punkt $P \in C$ mit $\phi(P) = Q$.
Fall $Q = (1 : a)$: In Q ist $t - a$ uniformisierend, genauer $(1 : t) \mapsto t - a$, also ist $\phi^*(t - a) = f - a$ und daher

$$e_\phi(P) = v_P(f - a).$$

Ist $a = 0$, so ist $e_\phi(P) = v_P(f)$ die Nullstellenordnung von f.
Fall $Q = (0 : 1)$: In Q ist $\frac{1}{t}$ uniformisierend, genauer $(1 : t) \mapsto \frac{1}{t}$, mit $\phi^*(\frac{1}{t}) = \frac{1}{f}$ gilt dann

$$e_\phi(P) = v_P(\frac{1}{f}) = -v_P(f).$$

Nun gilt der wichtige Satz, den wir ohne Beweis angeben:

SATZ 16. *Sei $\phi : C_1 \to C_2$ ein nichtkonstanter Morphismus zwischen glatten projektiven Kurven. Dann gilt:*

1. *Für alle $Q \in C_2$ ist*
$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi.$$
2. *Ist ϕ separabel, so gibt es nur endlich viele Verzweigungspunkte, insbesondere gilt für alle Punkte Q von C_2 mit nur endlich vielen Ausnahmen:*
$$\#\phi^{-1}(Q) = \deg \phi.$$

Jede nichtkonstante Funktion $f \in \overline{K}(C)$ liefert durch $\phi = (1 : f)$ einen Morphismus $\phi : C \to \mathbf{P}^1$, mit unserem letzten Beispiel folgt sofort:

FOLGERUNG 7. *Ist C eine glatte Kurve und $f \in \overline{K}(C) \setminus \overline{K}$, so nimmt f jeden Wert gleich oft an, wenn man mit Vielfachheiten zählt.*

Es gibt also genauso viele Null- wie Polstellen, womit wir haben:

FOLGERUNG 8. *Ist C eine glatte Kurve und $f \in \overline{K}(C)$, so gilt*

$$\sum_{P \in C} v_P(f) = 0.$$

Zum Schluß dieses Abschnittes wollen wir noch eine Klasse von Kurven einführen.

DEFINITION 25. *Eine nichtsinguläre Kurve C heißt hyperelliptisch, falls es einen nichtkonstanten Morphismus $\phi : C \to \mathbf{P}^1$ vom Grad 2 gibt.*

Wie kann man hyperelliptische Kurven beschreiben?

- Sei C eine hyperelliptische Kurve und $\phi = (1 : g)$ ein Morphismus vom Grad 2 auf $\mathbf{P}^1$. Außerdem sei die Charakteristik des Grundkörpers $\neq 2$.

- $\overline{K}(C)$ über $\phi^*\overline{K}(t)$ ist eine Körpererweiterung vom Grad 2, also gibt es ein $x \in \overline{K}(C)$, so daß $\overline{K}(C)$ Grad 2 über $\overline{K}(x)$ hat. Mithin gibt es ein quadratfreies Polynom $f(x)$ mit $\overline{K}(C) = \overline{K}(x)[\sqrt{f(x)}]$. Schreibt man $y = \sqrt{f(x)}$, so erhält man schließlich
$$\overline{K}(C) = \overline{K}(x,y) \text{ mit } y^2 = f(x).$$
- Damit ist C birational äquivalent zu der ebenen Kurve $C_0 \subseteq \mathbf{P}^2$ mit $y^2 = f(x)$. Man zeige, daß C_0 im Endlichen nichtsingulär ist.
- Im Unendlichen gibt es nur den Punkt $(0:0:1)$. Dieser ist singulär, falls $grad(f(x)) \geq 4$ ist.
- Der Morphismus hat jetzt die einfache Form $(x,y) \mapsto x$. Bei dem birationalen Morphismus $C \to C_0$ liegen über $(0:0:1)$ also einer oder zwei Punkte.

KAPITEL 4

Divisoren auf nichtsingulären Kurven

Im folgenden sei C eine nichtsinguläre (irreduzible) projektive Kurve über dem Körper K.

DEFINITION 26. 1. *Die Divisorengruppe $Div(C)$ von C ist die freie abelsche Gruppe, die von den Punkten auf C erzeugt wird. Ein Divisor $D \in Div(C)$ ist also eine formale Linearkombination*

$$D = \sum_{P \in C} n_P P$$

mit $n_P \in \mathbf{Z}$ und $n_P \neq 0$ für nur endlich viele Punkte von C.

2. *Der Grad $deg(D)$ eines Divisors $D = \sum n_P P$ ist $deg(D) = \sum n_P$.*
3. *Die Divisoren vom Grad 0 bilden eine Untergruppe:*

$$Div^0(C) = \{D \in Div(C) : deg(D) = 0\}.$$

4. *Die Galoisgruppe G_K operiert auf $Div(C)$ und $Div^0(C)$ durch*

$$\sigma(\sum n_P P) = \sum n_P(\sigma P).$$

5. *Man sagt, $D \in Div(C)$ ist über K definiert, falls $\sigma D = D$ für alle $\sigma \in G_K$ gilt. Sei $Div_K(C)$ bzw. $Div^0_K(C)$ die Gruppe der Divisoren bzw. Divisoren vom Grad 0, die über K definiert sind.*
6. *Ist $f \in \overline{K}(C)^\times$, so heißt*

$$(f) = div(f) = \sum v_P(f) P$$

der zu f gehörige Hauptdivisor.

Beispiel: Wir betrachten $\mathbf{P}^1$ mit t als Koordinate im Endlichen und $u = \frac{1}{t}$ im Unendlichen. Ein $f \in \overline{K}(\mathbf{P}^1), f \neq 0$ hat eine eindeutige Zerlegung

$$f = c\frac{(x-a_1)^{m_1}\dots(x-a_r)^{m_r}}{(x-b_1)^{n_1}\dots(x-b_s)^{n_s}},$$

mit $m_i, n_j \geq 1$, alle a_i, b_j verschieden. Im Unendlichen ist $v_\infty(f) = (\sum_j n_j) - (\sum_i m_i)$ und damit folgt

$$(f) = \sum_i m_i[a_i] - \sum_j n_j[b_j] + (\sum_j n_j - \sum_i m_i)\infty.$$

Insbesondere sieht man hier auch sofort $deg((f)) = 0$.

Beispiel: Wir betrachten die Kurve $C \subseteq \mathbf{P}^2$, die durch $y = x^2$ gegeben wird. Dann ist

$$(\sqrt{2}, 2) + (-\sqrt{2}, 2)$$

ein über $\mathbf{Q}$ definierter Divisor. Ist $\alpha^3 = 2$ und $\zeta = \frac{-1+\sqrt{-3}}{2}$ eine primitive dritte Einheitswurzel, so ist

$$(\alpha, \alpha^2) + (\zeta\alpha, \zeta^2\alpha^2) + (\zeta^2\alpha, \zeta\alpha^2)$$

ebenfalls über $\mathbf{Q}$ definiert.

LEMMA 5. *Seien $f, g \in \overline{K}(C)^\times$. Dann gilt:*

1. *$(fg) = (f) + (g)$, die Hauptdivisoren bilden also eine Untergruppe.*
2. *$(f) = 0 \iff f \in \overline{K}^\times$.*
3. *$(f) = (g) \iff f = cg$ für ein $c \in \overline{K}$.*
4. *$deg((f)) = 0$, d.h. Hauptdivisoren haben Grad 0.*

Beweis:

1. Dies folgt sofort aus $v_P(fg) = v_P(f) + v_P(g)$.
2. $(f) = 0$ heißt, f hat weder Pol- noch Nullstellen. Da ein nichtkonstantes $f \in \overline{K}(C)$ aber einen surjektiven Morphismus $\phi : C \to \mathbf{P}^2$ mit $\phi = (1 : f)$ liefert, ist klar, daß $(f) = 0$ mit $f \in \overline{K}(C)$ äquivalent ist.
3. Es gilt $(f) = (g)$ genau dann, wenn $0 = (f) - (g) = (\frac{f}{g})$, woraus mit der letzten Aussage die Behauptung folgt.
4. Aus dem letzten Abschnitt wissen wir: $\sum_P (f) = 0$, also $deg((f)) = 0$. ■

Beispiel: Seien $e_1, e_2, e_3 \in \overline{K}$ paarweise verschieden, $char(K) \neq 2$. Dann definiert $y^2 = (x - e_1)(x - e_2)(x - e_3)$ eine nichtsinguläre Kurve $C \subseteq \mathbf{P}^2$ mit einem unendlich fernen Punkt $P_\infty = (0 : 0 : 1)$. Sei $P_i = (e_i, 0)$. In P_1 ist $x - e_1 = 0$ Tangente, also y uniformisierend, außerdem $(x - e_2)(x - e_3)$ Einheit. Daher

$$2 = v_{P_1}(y^2) = v_{P_1}((x - e_1)(x - e_2)(x - e_3)) = v_{P_1}(x - e_1).$$

Da $x - e_1$ höchstens in P_1 eine Nullstelle hat, höchstens in P_∞ eine Polstelle hat, folgt

$$((x - e_1)) = 2P_1 - 2P_\infty.$$

Analog

$$(x - e_2) = 2P_2 - 2P_\infty \text{ und } (x - e_3) = 2P_3 - 2P_\infty.$$

Daraus ergibt sich $(y^2) = 2P_1 + 2P_2 + 2P_3 - 6P_\infty$, also

$$(y) = P_1 + P_2 + P_3 - 3P_\infty.$$

Definition 27. *Zwei Divisoren $D_1, D_2 \in Div(C)$ heißen linear äquivalent, $D_1 \sim D_2$, wenn es einen Hauptdivisor (f) gibt mit*

$$D_2 = D_1 + (f).$$

Die Picardgruppe oder Divisorenklassengruppe $Pic(C)$ ist der Quotient von $Div(C)$ modulo den Hauptdivisoren. Entsprechend definiert man

$$Pic^0(C) = \{ \text{ Divisoren vom Grad } 0\}/\{ \text{ Hauptdivisoren } \}.$$

Sei weiter

$$Pic_K(C) = \{c \in Pic(C) : \sigma c = c \text{ für alle } \sigma \in G_K\}$$

und analog $Pic^0_K(C)$.

Bemerkungen:

1. $Pic^0(C) = 0$ heißt, daß jeder Divisor vom Grad 0 Hauptdivisor ist. $Pic^0(C)$ mißt also, wieweit Divisoren vom Grad 0 von Hauptdivisoren abweichen. Man vergleiche die Funktion der Klassengruppe von Zahlkörpern.
2. Da Hauptdivisoren Grad 0 haben, erhalten wir durch die Gradfunktion eine induzierte Abbildung $deg : Pic(C) \to \mathbf{Z}$. Der Kern ist $Pic^0(C)$. Man kann dies auch mit der exakten Sequenz schreiben:

$$0 \to Pic^0(C) \to Pic(C) \to \mathbf{Z} \to 0.$$

Ist $P_0 \in C$, so definiert $(D_0, n) \mapsto D_0 + nP_0$ einen Isomorphismus von abelschen Gruppen

$$Pic^0(C) \oplus \mathbf{Z} \simeq Pic(C),$$

der von der Auswahl des Punktes P_0 abhängt.

Der folgende Satz gibt einen ersten Hinweis, wie wichtig $Pic(C)$ für die Klassifikation von Kurven ist:

Satz 17. *Für eine Kurve C sind äquivalent:*

1. $C \simeq \mathbf{P}^1$,
2. $Pic^0(C) = 0$,
3. *Es gibt ein $f \in \overline{K}(C)$ mit $(f) = P_1 - P_2$ und $P_1 \neq P_2$.*

Beweis:
1 ⇒ 2: Jeder Divisor D vom Grad 0 kann geschrieben werden

$$D = \sum_i m_i[a_i] - \sum_j n_j[b_j] + (\sum_j n_j - \sum_i m_i)[\infty]$$

mit $m_i, n_j \geq 0$. Offensichtlich gilt nun für

$$f = \frac{(x-a_1)^{m_1} \dots (x-a_r)^{m_r}}{(x-b_1)^{n_1} \dots (x-b_s)^{n_s}}$$

$(f) = D$, also ist D Hauptdivisor und damit $Pic^0(C) = 0$.
2 ⇒ 3: Wähle zwei verschiedene Punkte $P_1, P_2 \in C$. Dann hat $P_1 - P_2$ Grad 0, also gibt es eine Funktion f mit $(f) = P_1 - P_2$.
3 ⇒ 1: f induziert einen Morphismus $C \to \mathbf{P}^1$ vom Grad

$$deg(f) = \sum_{f(P)=0} v_P(f) = 1,$$

also ist $\overline{K}(C) = \overline{K}(f) \simeq \overline{K}(\mathbf{P}^1)$ und damit $C \simeq \mathbf{P}^1$. ∎

Wir wollen jetzt wichtige Beispiele von Divisoren kennenlernen.

Hyperebenenschnitte: Sei $C \subseteq \mathbf{P}^n$ und C nicht in einem echten Teilraum von $\mathbf{P}^n$ enthalten. Sei $\ell = a_0x_0 + \dots + a_nx_n = 0$ die Gleichung einer Hyperebene. Wir wollen den Divisor (ℓ) definieren: den Hyperebenenschnitt $\{\ell = 0\} \cap C$.
Sei $P \in C$. Ist $P \in U_i = \{x_i \neq 0\}$, so sei $n_P = v_P(\frac{\ell}{x_i}$. Ist P auch in U_j, so ist

$$v_P(\frac{\ell}{x_i}) = v_P(\frac{\ell}{x_j})$$

wegen $v_P(\frac{x_i}{x_j}) = 0$, d.h. n_P ist wohldefiniert. Nun setzt man

$$(\ell) = \sum_{P \in C} n_P P.$$

Ist $\ell' = 0$ eine andere Hyperebene, so ist $\frac{\ell}{\ell'}$ eine rationale Funktion auf C, und man sieht sofort, daß die Hyperebenenschnitte (ℓ) und (ℓ') linear äquivalent sind. Man nennt $deg((\ell))$ den Grad der Kurve C im $\mathbf{P}^n$.

Beispiele:
1. Sei $C = \{x_0x_2 = x_1^2\} \subseteq \mathbf{P}^2$. Je zwei Punkte auf C bilden einen Hyperebenenschnitt.
2. Für die Kurve C in affiner Darstellung $y^2 = x^3 - x$ bestehen die Hyperebenenschnitte aus 3 Punkten, die auf einer Geraden liegen.

Sei nun $\phi : C_1 \to C_2$ ein nichtkonstanter Morphismus glatter projektiver Kurven. Wir definieren

$$\phi^* : Div(C_2) \to Div(C_1), \quad Q \mapsto \sum_{P \in \phi^{-1}(P)} e_\phi(P) \text{ und lineare Fortsetzung,}$$

$$\phi_* : Div(C_1) \to Div(C_2), \quad P \mapsto \phi(P) \text{ und lineare Fortsetzung.}$$

Beispiel: Interpretieren wir eine nichtkonstantes $f \in \overline{K}(C)$ als $f : C \to \mathbf{P}^1$, so gilt

$$(f) = f^*((0) - (\infty)).$$

SATZ 18. *Sei $\phi : C_1 \to C_2$ ein Morphismus glatter projektiver Kurven. Dann gilt*
1. $deg(\phi^* D) = \deg \phi \cdot deg D$
2. $\phi^*(div(f)) = div(\phi^*(f))$
3. $deg(\phi_* D) = deg(D)$
4. $\phi_* \circ \phi^* = deg(\phi)$, *d.h. Multiplikation mit $deg(\phi)$ auf $Div(C_2)$.*

Der Beweis ergibt sich unmittelbar aus den Definitionen und früher erwähnten Eigenschaften.

KAPITEL 5

Differentialformen auf nichtsingulären Kurven

Sei wieder C eine nichtsinguläre irreduzible projektive Kurve.

Definition 28. *Der Raum Ω_C der meromorphen Differentialformen auf C ist der $\overline{K}(C)$-Vektorraum, der von Symbolen df mit $f \in \overline{K}(C)$ erzeugt wird, zusammen mit den Relationen*

$$d(f+g) = df + dg, \quad d(fg) = fdg + gdf, \quad dc = 0 \text{ für alle } c \in \overline{K}.$$

Jedes $\omega \in \Omega_C$ hat also eine Darstellung

$$\omega = \sum_{i=1}^{n} f_i dg_i \text{ mit } f_i g_i \in \overline{K}(C).$$

Wir üben etwas den Umgang mit den Differentialen: Seien $f, g \in \overline{K}(C)$.

- $d(f^2) = fdf + fdf = 2fdf$ und induktiv dann
$$d(f^n) = nf^{n-1}df \text{ für alle natürlichen Zahlen } n.$$
- Ist $f \neq 0$, so gilt:
$$0 = d(1) = d(f \cdot \frac{1}{f}) = fd(\frac{1}{f}) + \frac{1}{f}df,$$
woraus sofort
$$d(\frac{1}{f}) = -\frac{1}{f^2}df$$
folgt. Wie üblich erhält man dann
$$d(\frac{f}{g}) = \frac{gdf - fdg}{g^2}.$$
- Ist $F = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ ein Polynom mit $a_i \in \overline{K}$, so können wir die formale Ableitung $F' = \sum i a_i x^{i-1}$ bilden. Setzt man f ein, so erhält man
$$dF(f) = d(\sum a_i f^i) = \sum i a_i f^{i-1} df = F'(f)df.$$
Ist G ein weiteres Polynom mit $G(f) \neq 0$, so ist
$$d(\frac{F(f)}{G(f)}) = \frac{F'(f)G(f) - F(f)G'(f)}{G(f)^2}df.$$

Beispiel: Wegen $\overline{K}(\mathbf{P}^1) = \overline{K}(t)$ folgt aus den obigen Betrachtungen sofort, daß jedes $\omega \in \Omega_{\mathbf{P}^1}$ die Form

$$\omega = \frac{p(t)}{q(t)}dt$$

hat, mit Polynomen p und q.

Satz 19. *Ω_C ist ein 1-dimensionaler $\overline{K}(C)$-Vektorraum.*

Beweisidee: Der Funktionenkörper $\overline{K}(C)$ kann erzeugt werden von Elementen x und y mit einer Relation $f(x,y) = 0$. Wie oben überlegt man sich

$$\Omega_C = \overline{K}(C)dx + \overline{K}(C)dy.$$

Wir differenzieren jetzt die Relation $f(x,y) = 0$:

$$0 = d0 = d(f(x,y)) = \frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy.$$

Sei o.E. $\frac{\partial f}{\partial y} \neq 0$. Dann ist

$$dy = -\frac{\frac{\partial f}{\partial x}}{\frac{\partial f}{\partial y}} dx,$$

also $\Omega_C = \overline{K}(C)dx$. Zu zeigen bliebe noch, daß $\Omega_C \neq 0$ gilt, worauf wir aber verzichten. ■

Bemerkung: Für $c \in \overline{K}$ gilt $dc = 0$. In Charakteristik p gilt außerdem $d(f^p) = 0$ für jede Funktion f.

Ohne Beweis geben wir folgenden Satz an, der die von uns benötigten Aussagen enthält:

SATZ 20. 1. *Ist $char(K) = 0$, so gilt für $f \in \overline{K}(C)$:*

$$df = 0 \iff f \in \overline{K}.$$

2. *Ist $P \in C$ und t uniformisierend in P, so ist $dt \neq 0$, insbesondere $\Omega_C = \overline{K}(C)dt$.*

Ist also t uniformisierend in $P \in C$ und $f \in \overline{K}(C)$, so gibt es eine Funktion $g \in \overline{K}(C)$ mit $df = gdt$. Wir schreiben dann auch manchmal $g = \frac{df}{dt}$. Ohne Beweis geben wir folgendes Lemma an:

LEMMA 6. *Ist t uniformisierend in $P \in C$ und $f \in \overline{K}(C)$ definiert in P, so ist $\frac{df}{dt}$ auch definiert in P.*

DEFINITION 29. 1. *Ist $\omega \in \Omega_C, \omega \neq 0$, $P \in C$ und t uniformisierend in P, so gibt es eine Funktion g mit $\omega = gdt$. Man definiert*

$$v_P(\omega) = v_P(g).$$

Man sagt, ω ist holomorph oder regulär in P, falls $v_P(\omega) \geq 0$ ist.

2. *Der Divisor eines Differentials $\omega \in \Omega_C$ wird wie folgt definiert:*

$$(\omega) = \sum_{P \in C} v_P(\omega)P.$$

Den Divisor eines Differentials nennt man auch einen kanonischen Divisor.

Bemerkung: Man kann jetzt leicht zeigen, daß die Definition von $v_P(\omega)$ nicht von der Auswahl der Uniformisierenden in P abhängt.

Beispiel: $C = \mathbf{P}^1$ und $\omega = dt$. Was ist (dt)? Im Endlichen: In einem Punkt a ist $t - a$ uniformisierend, wegen $dt = d(t-a) = 1 \cdot d(t-a)$ gilt also $v_{[a]}(dt) = 0$. Im unendlich fernen Punkt ∞ ist $u = \frac{1}{t}$ uniformisierend, mit

$$dt = d(\frac{1}{u}) = -\frac{1}{u^2}du = (-1)u^{-2}du$$

gilt also $v_\infty(dt) = -2$, womit man schließlich erhält:

$$(dt) = -2\infty \quad \text{und} \quad deg((dt)) = -2.$$

Sind ω_1 und ω_2 zwei von 0 verschiedene Differentiale, so gibt es eine Funktion f mit $\omega_2 = f\omega_1$. Ist t uniformisierend in P und g_i mit $\omega_i = g_i dt$, so gilt $g_2 = fg_1$ und damit

$$v_P(\omega_2) = v_P(g_2) = v_P(f) + v_P(g_1) = v_P(f) + v_P(\omega_1),$$

was für die Divisoren sofort

$$(\omega_2) = (f) + (\omega_1)$$

liefert. Die Divisoren zweier Differentialformen sind also linear äquivalent. Umgekehrt sieht man sofort: Ist ein Divisor linear äquivalent zu einem kanonischen Divisor, so ist er selbst schon ein kanonischer Divisor. Die Äquivalenzklasse der kanonischen Divisoren in $Pic(C)$ nennt man die kanonische Klasse k_C von C.

Beispiel: Wir betrachten die (nichtsinguläre) Kurve $C \subseteq \mathbf{P}^2$, die durch die Gleichung $y^2 = x^3 - x$ definiert wird. Also $C = \{x_0x_2^2 = x_1^3 - x_0^2x_1\}$. Wir wollen den Divisor des Differentials $\omega = dx$ berechnen. *Im Endlichen:* Sei $P_1 = (-1,0), P_2 = (0,0), P_3 = (1,0)$. Sei $P = (a,b) \in C$. Ist $P \neq P_i$, so ist $x - a$

uniformisierend, wegen $dx = d(x-a)$ also $v_P(\omega) = 0$. In P_i ist y uniformisierend. Wir differenzieren $y^2 = x^3 - x$ und erhalten

$$2ydy = (3x^2-1)dx \quad \text{und} \quad \omega = dx = \frac{2y}{3x^2-1}dy.$$

In P_i ist $3x^2-1$ Einheit, also gilt $v_{P_i}(\omega) = 1$.
Im Unendlichen: Es gibt nur den einen Punkt $P_\infty = (0:0:1)$. Wir wählen affine Koordinaten u, v mit $(u:v:1) = (x_0:x_1:x_2) = (1:x:y)$ und haben dann die Gleichung $u = v^3 - u^2v$. In P_∞ ist v uniformisierend und $v_{P_\infty}(u) = 3$. Zunächst gilt nun $\omega = dx = d(\frac{u}{v}) = \frac{1}{u}dv - \frac{v}{u^2}du$. Durch Differenzieren der Gleichung $u = v^3 - u^2v$ erhält man $(1+2uv)du = (3v^2-u^2)dv$ und damit

$$\omega = dx = \frac{-2-4uv}{u(1+2uv)}dv,$$

woraus man sofort $v_{P_\infty}(\omega) = -3$ ablesen kann. Also gilt

$$(\omega) = P_1 + P_2 + P_3 - 3P_\infty.$$

Den gleichen Divisor hat die Funktion y: $(dx) = (y)$ und damit

$$(\frac{1}{y}dx) = 0.$$

Damit gilt $k_C = 0$.

Zur Übung rechne man in gleicher Weise folgendes Beispiel:

Beispiel: Seien $e_1, e_2, e_3 \in \overline{K}$ paarweise verschieden und $C \subseteq \mathbf{P}^2$ gegeben durch die affine Gleichung $y^2 = (x-e_1)(x-e_2)(x-e_3)$. Mit $A = e_1+e_2+e_3$, $B = e_1e_2 + e_1e_3 + e_2e_3$ und $C = e_1e_2e_3$ können wir auch $y^2 = x^3 - Ax^2 + Bx - C$ schreiben bzw. projektiv $x_0x_2^2 = x_1^3 - Ax_0x_1^2 + Bx_0^2x_1 - Cx_0^3$. Wir wollen den kanonischen Divisor (dx) berechnen. Sei $P_i = (e_i, 0)$ und $P_\infty = (0:0:1)$.
Im Endlichen: Ist $P = (a,b) \neq P_i$, so ist $x-a$ uniformisierend, wegen $dx = d(x-a)$ also $v_P(dx) = 0$. In P_i ist y uniformisierend. Wir differenzieren die Definitionsgleichung $y^2 = x^3 - Ax^2 + Bx - C$:

$$2ydy = (3x^2 - 2Ax + B)dx.$$

In P_i ist $(3x^2-2Ax+B)(P_i) = (e_i-e_j)(e_i-e_k) \neq 0$ (i,j,k paarweise verschieden), $3x^2-2Ax+B$ also Einheit und damit $v_{P_i}(dx) = 1$.
Im Unendlichen: Wir verwenden affine Koordinaten u, v mit $(u:v:1) = (1:x:y)$, also $x = \frac{v}{u}, y = \frac{1}{u}$. Die Gleichung lautet $u = v^3 - Auv^2 + Bu^2v - Cu^3$. Die Tangente in P_∞ ist also $u = 0$, mithin v uniformisierend. Aus der Gleichung sieht man dann sofort $v_\infty(u) = 3$. Durch Differenzieren der Gleichung erhält man

$$(1 + 3Cu^2 - 2Buv + Av^2)du = (Bu^2 - 2Auv + 3v^2)dv,$$

und daher mit $dx = d(\frac{v}{u}) = \frac{1}{u}dv - \frac{v}{u^2}du$

$$dx = \frac{3Auv^2 - 3Bu^2v + 3Cu^3 + u - 3v^3}{u^2(Av^2 - 2Buv + 3Cu^2 + 1)}dv.$$

Nun gilt $v_\infty(u - 3v^3) = 3$, so daß sich $v_\infty(dx) = -3$ ergibt.
Insgesamt haben wir also

$$(dx) = P_1 + P_2 + P_3 - 3P_\infty.$$

Diesen Divisor kennen wir bereits: $(dx) = (y)$ und damit $(\frac{dx}{y}) = 0$. Das Differential $\frac{dx}{y}$ hat also weder Pol- noch Nullstellen. Außerdem gilt $k_C = 0$.

Die folgende Definition führt eine zentrale Invariante ein:

DEFINITION 30. *Das Geschlecht g (oder $g(C)$ oder g_C) einer Kurve C wird definiert durch die Formel*

$$2g - 2 = deg(k_C),$$

wo k_C die kanonische Klasse bezeichnet.

Beispiele:

1. Wegen $k_{\mathbf{P}^1} = -2$ hat $\mathbf{P}^1$ Geschlecht 0.

2. Die vorhin betrachteten Kurven $y^2 = (x-e_1)(x-e_2)(x-e_3)$ (alle e_i's verschieden) haben $k_C = 0$, also Geschlecht 1.

Adjunktionsformel für glatte ebene Kurven:

- Sei $C \subseteq \mathbf{P}^2$ eine nichtsinguläre Kurve vom Grad d, d.h. gegeben durch ein Polynom $f(x,y) = 0$ bzw. homogen $x_0^d f(\frac{x_1}{x_0}, \frac{x_2}{x_0}) = 0$.
- Im Funktionenkörper gilt $f(x,y) = 0$, woraus folgt $\frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy = 0$ und daher
$$\omega = \frac{dx}{\frac{\partial f}{\partial y}} = -\frac{dy}{\frac{\partial f}{\partial x}}.$$
- Wir betrachten ω im Endlichen, in einem Punkt $P = (a,b)$.
  Ist $\frac{\partial f}{\partial y}(P) \neq 0$, so ist $x-a$ uniformisierend und mit $d(x-a) = dx$ folgt $v_P(\omega) = 0$.
  Ist $\frac{\partial f}{\partial x}(P) \neq 0$, so ist $y-b$ uniformisierend und mit $d(y-b) = dy$ ergibt sich $v_P(\omega) = 0$.
- Im Unendlichen: Wir nehmen an, $(0:1:0)$ liegt nicht auf der Kurve, dann liegen alle unendlich fernen Punkte von C im affinen Teil $\{(u:v:1)\}$ und zwar auf $u = 0$. Wegen $(1:x:y) = (u:v:1) = (1:\frac{v}{u}:\frac{1}{u})$ gilt im Funktionenkörper $x = \frac{v}{u}$ und $y = \frac{1}{u}$. Die Ableitung $\frac{\partial f}{\partial x}$ hat Grad $d-1$, also ist $g(u,v) = u^{d-1}\frac{\partial f}{\partial x}(\frac{v}{u}, \frac{1}{u})$ ein Polynom in u und v. Mit $dy = d(\frac{1}{u}) = -\frac{1}{u^2}du$ erhalten wir
$$\omega = -\frac{dy}{\frac{\partial f}{\partial x}} = \frac{u^{d-3}du}{g(u,v)}.$$
- Nun kann man erreichen, daß der Geradenschnitt (x_0) aus d verschiedenen Punkten besteht:
$$(x_0) = P_1 + \cdots + P_d.$$
  Dann ist u uniformisierend in P_i und $v_{P_i}(\omega) = d-3$.
- Man erhält also
$$(\omega) = (d-3)P_1 + \cdots + (d-3)P_d = (d-3)(x_0).$$
  Insbesondere ist $deg(k_C) = d(d-3)$.
- Aufgabe: Verifiziere die fürs Unendliche gemachten Aussagen durch explizites Ausrechnen.

Damit erhalten wir folgenden Satz:

Satz 21. *Sei $C \subseteq \mathbf{P}^2$ eine nichtsinguläre Kurve vom Grad d. Ist h die Klasse eines Hyperebenenschnitts, so gilt für die kanonische Klasse*
$$k_C = (d-3)h,$$
also $deg k_C = d(d-3)$ und damit $g_C = \frac{(d-1)(d-2)}{2}$.

Was passiert, wenn eine ebene Kurve C Singularitäten hat? Durch Aufblasen erhalten wir eine nichtsinguläre birational äquivalente Kurve $\tilde{C}$. Welches Geschlecht hat $\tilde{C}$? Natürlich kann man dies bei einer konkret gegebenen Kurve ausrechnen, indem man den Divisor eines Differentials bestimmt. In vielen Fällen kann man aber auch obige Betrachtung modifizieren und erhält eine Aussage über das Geschlecht.

Definition 31. *Ein Punkt $P = (x_0, y_0)$ einer ebenen Kurve $f(x,y) = 0$ heißt einfacher Knoten oder gewöhnlicher Doppelpunkt, falls die Taylorreihenentwicklung in P folgende Gestalt hat:*
$$f = a(x-x_0)^2 + b(x-x_0)(y-y_0) + c(y-y_0)^2 + \ldots \qquad \text{mit } b^2 - 3ac \neq 0.$$

Nach Koordinatenwechsel sieht also die Taylorreihenentwicklung in einem einfachen Knoten wie folgt aus:
$$f = xy + \ldots$$

Damit gilt jetzt folgender Satz:

Satz 22. *Sei $C \subseteq \mathbf{P}^2$ eine irreduzible projektive Kurve vom Grad d mit nur einfachen Knoten als Singularitäten, und zwar δ Stück. Ist $\tilde{C}$ eine glattes Modell von C, so gilt*
$$g(\tilde{C}) = \frac{(d-1)(d-2)}{2} - \delta.$$

Beweisskizze: Wir können annehmen, daß alle Singularitäten im Endlichen liegen. $\tilde{C}$ werde durch Aufblasung in den Singularitäten erhalten. Wir betrachten wieder das Differential

$$\omega = \frac{dx}{\frac{\partial f}{\partial y}} = -\frac{dy}{\frac{\partial f}{\partial x}}.$$

Wir müssen nur sehen, was in den singulären Punkten passiert. O.E. sei $P = (0,0)$ ein einfacher Knoten von C.

- Sei $f = xy + \sum_{i\geq 3} g_i(x,y)$, wo $g_i(x,y)$ homogen vom Grad i ist.
- Wir blasen $\mathbf{A}^2$ auf in $(0,0)$ und erhalten $X = \{((x,y),(u:v)) \in \mathbf{A}^2 \times \mathbf{P}^1 : xv = yu\}$. Die exzeptionelle Faser sei E, das eigentliche Urbild von C sei $\tilde{C}$. Uns interessiert also, was in den Punkten $E \cap \tilde{C}$ von $\tilde{C}$ passiert. Dazu betrachten wir zwei affine Teile von X:
- $u = 1$: Dann hat man $y = xv$ und die Koordinaten x, v. Einsetzen liefert
$$f = x^2v + \sum_{i\geq 3} g_i(x,xv) = x^2v + \sum_{i\geq 3} x^i g_i(1,v),$$
so daß hier das eigentliche Urbild $\tilde{C}$ gegeben wird durch
$$v + \sum_{i\geq 3} x^{i-2} g_i(1,v) = 0.$$
$E \cap \tilde{C} \cap \{u = 1\}$ besteht nur aus dem Punkt $P_1 = ((0,0),(1:0))$.
- Der Punkt P_1 ist nichtsingulär auf $\tilde{C}$ und x ist uniformisierend. Was passiert mit $\omega = dx/\frac{\partial f}{\partial y}$? Wir haben
$$\frac{\partial f}{\partial y} = x + \sum_{i\geq 3} \frac{\partial g_i}{\partial y}(x,y) = x + \sum_{i\geq 3} \frac{\partial g_i}{\partial y}(x,xv),$$
woraus sofort $v_{P_1}(\frac{\partial f}{\partial y}) = 1$ folgt, also
$$v_{P_1}(\omega) = -1.$$
- Im affinen Teil $v = 1$ findet man den Punkt $P_2 = ((0,0),(0:1))$ und analog $v_{P_2}(\omega) = -1$.
- Die Singularität erniedrigt also den Grad des kanonischen Divisors um 2, das Geschlecht erniedrigt sich also um 1, was wir zeigen wollten. ■

Definition 32. *Sei $\phi : C_1 \to C_2$ ein nichtkonstanter Morphismus zwischen glatten projektiven Kurven. Dann definieren wir*

$$\phi^* : \Omega_{C_2} \to \Omega_{C_1} \text{ durch } \phi^*(\sum f_i dg_i) = \sum (\phi^* f_i) d(\phi^* g_i).$$

Da Ω_C ein 1-dimensionaler $\overline{K}(C)$-Vektorraum ist, ist $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ entweder injektiv oder identisch 0. Der folgende Satz gibt die wesentliche Charakterisierung.

Satz 23. *$\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ ist genau dann injektiv, wenn $\phi : C_1 \to C_2$ separabel ist.*

Wir werden diesen Satz nicht beweisen, geben aber ein Beispiel für das wesentliche Phänomen:

Beispiel: Hat K Charakteristik p und ist $\phi : \mathbf{P}^1 \to \mathbf{P}^1$ gegeben durch $t \mapsto t^p$ oder $\phi = (1 : t^p)$, so gilt für das Differential $\omega = f(t)dt$:

$$\phi^*\omega = f(t^p)d(t^p) = f(t^p)pt^{p-1}dt = 0,$$

also ist $\phi^* : \omega_{\mathbf{P}^1} \to \omega_{\mathbf{P}^1}$ in diesem Fall die 0-Abbildung.

Riemann-Hurwitz-Formel: Sei $\phi : C_1 \to C_2$ ein separabler Morphismus und ω eine Differentialform auf C_2. Wir wollen

$$div(\phi^*\omega) \text{ und } \phi^*(div(\omega))$$

vergleichen.

- Sei $P \in C_1$ und $Q = \phi(P)$. Sei s uniformisierend in Q, also $\omega = us^m ds$ mit $m = v_Q(\omega)$.
- Sei t uniformisierend in P, $e = e_\phi(P)$ der Verzweigungsindex, also $\phi^* s = vt^e$ mit einer Einheit v. Dann gibt es auch eine in P definierte Funktion g mit $dv = gdt$.

- Wir betrachten $\phi^*\omega$ in P:

$$\begin{aligned}\phi^*\omega &= \phi^*(us^m)d(\phi^*s) = \phi^*u \cdot v^m \cdot t^{em} \cdot d(vt^e) = \\ &= \phi^*u \cdot v^m \cdot t^{em} \cdot (t^e dv + vd(t^e)) = \phi^*u \cdot v^m \cdot t^{em} \cdot (t^e gdt + evt^{e-1}dt) = \\ &= \phi^*u \cdot v^m \cdot t^{em} \cdot (t^e g + evt^{e-1})dt\end{aligned}$$

Wir haben jetzt zwei Fälle:
1. Fall: $e \neq 0$ in K: Dann gilt

$$v_P(\phi^*\omega) = me + e - 1 = e_\phi(P)v_Q(\omega) + (e_\phi(P) - 1).$$

2. Fall: $e = 0$ in K: Dann ist

$$v_P(\phi^*\omega) > e_\phi(P)v_Q(\omega) + (e_\phi(P) - 1).$$

- Seien jetzt alle Verzweigungsindizes $e_\phi(P) \neq 0$ in K. Dann gilt:

$$\begin{aligned}div(\phi^*\omega) &= \sum_{P\in C_1} v_P(\phi^*\omega)P = \\ &= \sum_{P\in C_1} e_\phi(P)v_Q(\omega)P + (e_\phi(P)-1)P = \\ &= \sum_{Q\in C_2}\ \sum_{P\in C_1, \phi(P)=\mathbf{Q}} e_\phi(P)v_Q(\omega)P + \sum_{P\in C_1}(e_\phi(P)-1)P = \\ &= \sum_{Q\in C_2} v_Q(\omega)\phi^*Q + \sum_{P\in C_1}(e_\phi(P)-1)P = \\ &= \phi^*(\sum_{Q\in C_2} v_Q(\omega)Q) + \sum_{P\in C_1}(e_\phi(P)-1)P = \\ &= \phi^*(div(\omega)) + \sum_{P\in C_1}(e_\phi(P)-1)P.\end{aligned}$$

- In der letzten Formel berechnen wir noch die Grade und erhalten

$$2g(C_1) - 2 = deg(\phi)(2g(C_2) - 2) + \sum_{P\in C_1}(e_\phi(P) - 1).$$

Damit erhalten wir folgenden Satz, der auch als Riemann-Hurwitz-Formel bezeichnet wird:

SATZ 24. *Sei $\phi : C_1 \to C_2$ separabler Morphismus und alle Verzweigungsindizes $e_\phi(P) \neq 0$ in K. Ist ω ein Differential in C_2, so gilt*

$$div(\phi^*\omega) = \phi^*(div(\omega)) + \sum_{P\in C_1}(e_\phi(P) - 1),$$

woraus sich für die Geschlechter der Kurven ergibt:

$$2g(C_1) - 2 = deg(\phi)(2g(C_2) - 2) + \sum_{P\in C_1}(e_\phi(P) - 1).$$

Der Divisor $\sum_{P\in C_1}(e(_\phi(P) - 1)$ heißt auch der Verzweigungsdivisor von ϕ.

Beispiel: Sei C eine hyperelliptische Kurve in Charakteristik $\neq 2$. D.h. es gibt einen Morphismus $\phi : C \to \mathbf{P}^1$ vom Grad 2. ϕ sei in den Punkten $P_1, \ldots, P_n$ verzweigt. Dann ist $e_\phi(P_i) = 2$. Bezeichnet C das Geschlecht von C, so liefert die Riemann-Hurwitz-Formel $2g - 2 = 2 \cdot (-2) + n$ oder

$$g = \frac{n-2}{2}.$$

(Wir werden später sehen, daß das Geschlecht immer eine ganze Zahl ≥ 0 ist, was hier liefert, daß die Zahl der Verzweigungspunkte n gerade ist.)

Aufgabe: Konstruiere für kleines g Beispiele für Kurven vom Geschlecht g.

KAPITEL 6

Der Satz von Riemann-Roch

Sei im folgenden C eine nichtsinguläre irreduzible projektive Kurve über K.

DEFINITION 33. *Für zwei Divisoren* $D_1 = \sum m_P P$ *und* $D_2 = \sum n_P P$ *auf* C *definiert man:*

$$D_1 \geq D_2 \quad \Longleftrightarrow \quad m_P \geq n_P \text{ für alle } P \in C.$$

Ein Divisor $D = \sum n_P P \in Div(C)$ *heißt effektiv, falls* $D \geq 0$ *gilt, d.h.* $n_P \geq 0$ *für alle* $P \in C$.

Beispiel: Wie kann man ausdrücken, daß eine Funktion $f \in \overline{K}(C)^\times$ höchstens in P_0 eine Polstelle hat, und zwar höchstens von der Ordnung n? — Die Bedingungen lauten: $v_{P_0}(f) \geq -n$ und $v_P(f) \geq 0$ für alle $P \neq P_0$. Dies ist offensichtlich gleichwertig mit $(f) = \sum v_P(f) P \geq -nP_0$ oder auch: $(f) + nP_0 \geq 0$.

DEFINITION 34. *Für* $D \in Div(C)$ *sei*

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^\times : (f) + D \geq 0\} \cup \{0\}.$$

$\mathcal{L}(n_1P_1 + \cdots + n_rP_r)$ enthält also genau die Funktionen, die höchstens in den P_i's Pole haben, und zwar höchstens von der Ordnung n_i.

LEMMA 7. $\mathcal{L}(D)$ *ist ein* $\overline{K}$*-Vektorraum.*

Beweis: Sei $D = \sum n_P P$, $f, g \in \mathcal{L}(D)$ und $c \in \overline{K}, c \neq 0$. Dann gilt $v_P(f), v_P(g) \geq -n_P$ und damit

$$v_P(f+g) \geq \min(v_P(f), v_P(g)) \geq -n \text{ und } v_P(cf) = v_P(f) \geq -n,$$

also $f + g \in \mathcal{L}(D)$ und $cf \in \mathcal{L}(D)$. ■

DEFINITION 35. *Wir setzen* $\ell(D) = \dim_{\overline{K}} \mathcal{L}(D)$.

Eine fundamentale Aufgabe ist die Bestimmung von $\mathcal{L}(D)$ und die von $\ell(D)$.

Beispiel: Sei $C = \mathbf{P}^1$ und $n \geq 0$. Was ist dann $\mathcal{L}(n \cdot \infty)$? Jedes $f \in \overline{K}(t)^\times$ hat eine eindeutige Darstellung

$$f = c\frac{(t-a_1)^{m_1} \dots (t-a_r)^{m_r}}{(t-b_1)^{n_1} \dots (x-b_s)^{n_s}}$$

mit $m_i, n_j \geq 1$. Ist $s \geq 1$, so hat f eine Polstelle im Endlichen. Ist also $f \in \mathcal{L}(D)$, so muß f ein Polynom sein: $f = \sum c_i t^i$. Ist d der Grad von f, so ist $v_\infty(f) = -d$, was sofort

$$\mathcal{L}(n \cdot \infty) = \{ \text{ Polynome vom Grad } \leq n\}$$

liefert. Eine Basis dieses Vektorraums ist $1, t, t^2, \dots, t^n$, also ergibt sich außerdem

$$\ell(n \cdot \infty) = n + 1 = deg(n \cdot \infty) + 1.$$

SATZ 25. *Seien* D *und* D' *Divisoren auf* C. *Dann gilt:*

1. *Ist* $deg(D) < 0$, *so ist* $\mathcal{L}(D) = 0$ *und* $\ell(D) = 0$.
2. *Sind* D *und* D' *linear äquivalent, so gilt* $\mathcal{L}(D) \simeq \mathcal{L}(D')$ *und insbesondere* $\ell(D) = \ell(D')$.
3. *Ist* $D \leq D'$, *so* $\mathcal{L}(D) \subseteq \mathcal{L}(D')$ *und* $\ell(D) \leq \ell(D')$.
4. *Sei* $P \in C$ *und* $D \in Div(C)$. *Ist* $f \in \mathcal{L}(D+P) \setminus \mathcal{L}(D)$, *so gilt bereits* $\mathcal{L}(D+P) = \mathcal{L}(D) + \overline{K}f$. *Insbesondere ist* $\ell(D+P) \leq \ell(D) + 1$.
5. *Es ist* $\ell(D) < \infty$. *Genauer: Gilt* $deg(D) \geq 0$, *so ist* $\ell(D) \leq deg(D) + 1$.

Beweis:

1. Wäre $\mathcal{L}(D) \neq 0$, so gäbe es ein $f \in \mathcal{L}(D) \setminus \{0\}$. Dann ist $D + (f) \geq 0$, also folgt
$$deg(D) = deg(D) + deg((f)) = deg(D + (f)) \geq 0,$$
ein Widerspruch zur Annahme.
2. Sei $D' = D + (f)$. Dann gilt für $g \in \overline{K}(C)^\times$:
$$g \in \mathcal{L}(D') \iff D' + (g) \geq 0 \iff D + (f) + (g) \geq 0 \iff D + (fg) \geq 0 \iff fg \in \mathcal{L}(D),$$
also $f \cdot \mathcal{L}(D') = \mathcal{L}(D)$, woraus die Behauptung folgt.
3. Sei $D \leq D'$ und $f \in \mathcal{L}(D) \setminus \{0\}$. Dann gilt $D' + (f) \geq D + (f) \geq 0$, also $f \in \mathcal{L}(D')$. D.h. $\mathcal{L}(D) \subseteq \mathcal{L}(D')$.
4. Sei $D = nP + \dots$, d.h. n ist die Multiplizität von D in P. Sei t uniformisierend in P. Dann ist $v_P(ft^{n+1}) = 0$, also $(ft^{n+1})(P) \neq 0$. Ist jetzt $g \in \mathcal{L}(D + P)$, so gilt $v_P(gt^{n+1}) \geq 0$, also gibt es eine Konstante c mit $(gt^{n+1})(P) = c(ft^{n+1})(P)$, was $v_P(gt^{n+1} - cft^{n+1}) \geq 1$ und somit $v_P(g - cf) \geq -n$ liefert. Also gilt $g - cf \in \mathcal{L}(D)$ und damit $g \in \mathcal{L}(D) + \overline{K}f$ wie behauptet.
5. Wir können $deg(D) \geq 0$ und $\mathcal{L}(D) \neq 0$ voraussetzen. Dann gibt es ein f mit $D + (f) \geq 0$. Also ist $D' = D + (f)$ effektiv und $\ell(D') = \ell(D)$. Wir können uns also auf effektive Divisoren beschränken: $D' = P_1 + \dots + P_n$. Mit Hilfe der letzten Aussage ergibt sich
$$\ell(P_1 + \dots + P_n) \leq \ell(P_1 + \dots + P_{n-1}) + 1 \leq \dots \leq \ell(0) + n = n + 1,$$
was zu zeigen war. ■

Ohne Beweis geben wir jetzt folgenden fundamentalen Satz an:

SATZ 26 (Riemann-Roch). *Ist C eine Kurve vom Geschlecht g, so gilt für alle Divisoren $D \in Div(C)$:*
$$\ell(D) = deg(D) + 1 - g + \ell(K - D).$$

Beispiel: Wir wissen bereits $\mathcal{L}(0) = \overline{K}$, also $\ell(0) = 1$. Setzen wir dies in Riemann-Roch ein, so erhalten wir $1 = 0 + 1 - g + ell(K)$, also $\ell(K) = g$. Insbesondere bedeutet dies, daß das Geschlecht g eine ganze Zahl ≥ 0 ist. Setzen wir jetzt $D = K$ in Riemann-Roch ein, so erhalten wir: $g = deg(K) + 1 - g + \ell(0)$, also $deg(K) = 2g - 2$, was unsere Definition von Geschlecht war. Damit haben wir bewiesen:

FOLGERUNG 9.
$$\ell(K) = g \quad \textit{und} \quad deg(K) = 2g - 2.$$

Bemerkung: Sei $K = \omega$ mit einer Differentialform ω. Dann gilt für $f \in \overline{K}(C), f \neq 0$:
$$f \in \mathcal{L}(K) \iff (f) + (\omega) \geq 0 \iff (f\omega) \geq 0,$$
also
$$\mathcal{L}(K) \simeq \{ \text{ holomorphe Differentialformen auf } C\}.$$
Man deutet daher $\mathcal{L}(K)$ oft auch als Vektorraum der holomorphen Differentialformen auf C.

Beispiel: $C = \mathbf{P}^1$. Hier ist $K = -2\infty$. C hat Geschlecht 0. Sei D ein Divisor auf C vom Grad n. Dann ist $D \sim n\infty$. Also o.E. $D = n\infty$. Riemann-Roch lautet dann
$$\ell(n\infty) = n + 1 - \ell(-(n + 2)\infty).$$
Ist $n < 0$, so ist $\ell(n\infty) = 0$. Ist $n \geq 0$, so ist $\ell(-(n + 2)\infty) = 0$, also $\ell(n\infty) = n + 1$. Dies haben wir aber bereits explizit ausgerechnet.

Der Satz von Riemann-Roch berechnet zunächst nicht $\ell(D)$ in Abhängigkeit von $deg(D)$, denn ein Korrekturterm $\ell(K - D)$ ist erforderlich. Gilt aber $deg(K - D) < 0$, d.h. $deg(D) > 2g - 2$, so ist $\ell(K - D) = 0$ und Riemann-Roch ergibt $\ell(D) = deg(D) + 1 - g$. Damit haben wir gezeigt:

FOLGERUNG 10. *Für einen Divisor $D \in Div(C)$ gilt*
$$deg(D) > 2g - 2 \quad \Rightarrow \quad \ell(D) = deg(D) + 1 - g.$$

Beispiel: Sei $p \in C$. Für hinreichend großes n gilt dann $\ell(nP) = n + 1 - g$, d.h. es gibt Funktionen, die nur in P eine Polstelle haben.

Beispiel: Sei $C \subseteq \mathbf{P}^2$ definiert durch $y^2 = (x - e_1)(x - e_2)(x - e_3)$ mit drei verschiedenen Zahlen $e_1, e_2, e_3 \in \overline{K}$. C hat $K = 0$, Geschlecht 1 und einen Punkt im Unendlichen: $P = \infty = (0 : 0 : 1)$. Es gilt: $v_P(x) = -2, v_P(y) = -3$. Sei nun $n \geq 1$. Was ist $\mathcal{L}(nP)$? Wegen $\ell(K - nP) = \ell(-nP) = 0$ liefert Riemann-Roch $\ell(nP) = n$. Damit folgt

$$\begin{array}{rcl} \mathcal{L}(P) & = & \overline{K} \\ \mathcal{L}(2P) & = & \overline{K} + \overline{K}x \\ \mathcal{L}(3P) & = & \overline{K} + \overline{K}x + \overline{K}y \\ \mathcal{L}(4P) & = & \overline{K} + \overline{K}x + \overline{K}y + \overline{K}x^2 \\ \mathcal{L}(5P) & = & \overline{K} + \overline{K}x + \overline{K}y + \overline{K}x^2 + \overline{K}xy \\ \mathcal{L}(6P) & = & \overline{K} + \overline{K}x + \overline{K}y + \overline{K}x^2 + \overline{K}xy + \overline{K}x^3 \end{array}$$

Induktiv sieht man schnell, daß

$$1, x, x^2, , x^2, \ldots, x^{[\frac{n}{2}]}, y, xy, x^2y, \ldots, x^{[\frac{n-3}{2}]}y$$

eine Basis von $\mathcal{L}(nP)$ ist.

Bemerkung: Es gibt Verfahren, wie man explizit eine Basis von $\mathcal{L}(D)$ bestimmen kann.

Für uns ist folgende Aussage von Bedeutung:

Satz 27. *Ist $D \in Div_K(C)$ ein über K definierter Divisor, so besitzt $\mathcal{L}(D)$ eine Basis aus $K(C)$.*

Beweis: Es genügt zu zeigen: Jedes Element aus $\mathcal{L}(D)$ ist Linearkombination von Elementen von $\mathcal{L}(D) \cap K(C)$. Sei also $f \in \mathcal{L}(D)$. Dann gibt es eine endliche galoissche Körpererweiterung L von K mit $f \in L(C)$. Sei $G = Gal(L|K) = \{\sigma_1, \ldots, \sigma_n\}$ und $\alpha_1, \ldots, \alpha_n$ eine K-Basis von L. Wir definieren

$$g_i = \sigma_1(\alpha_i f) + \cdots + \sigma_n(\alpha_i f).$$

Da g_i invariant unter G ist, folgt $g_i \in K(C)$, also $g_i \in \mathcal{L}(D) \cap K(C)$. Nun haben wir

$$\begin{pmatrix} g_1 \\ \ldots \\ g_n \end{pmatrix} = \begin{pmatrix} \sigma_1\alpha_1 & \sigma_2\alpha_1 & \ldots & \sigma_n\alpha_1 \\ \ldots & \ldots & \ldots & \ldots \\ \sigma_n\alpha_1 & \sigma_n\alpha_2 & \ldots & \sigma_n\alpha_n \end{pmatrix} \begin{pmatrix} \sigma_1 f \\ \ldots \\ \sigma_n f \end{pmatrix}.$$

Die Matrix werde mit M bezeichnet. Dann ist $det(M)^2$ die Diskriminante von L über K, also $\neq 0$. Mithin ist $f = \sigma_1 f$ $\overline{K}$-Linearkombination von $g_1, \ldots, g_n$, was wir zeigen wollten. ■

Beispiel: Wir betrachten die Quadrik $Q \subseteq \mathbf{P}^2$, die affin durch die Gleichung

$$y + ax^2 + bxy + cy^2 = 0$$

mit $a \neq 0$ definiert wird. Der Grad ist 2, also hat Q Geschlecht 0. Wir haben den K-rationalen Punkt $P = (0,0)$ und wollen $\mathcal{L}(P)$ bestimmen. Nach Riemann-Roch ist $\ell(P) = 2$. Natürlich ist $\overline{K} \subseteq \mathcal{L}(P)$.
Im Endlichen: Im Funktionenkörper gilt $ax^2 = -y(1 + bx + cy)$, also

$$f = \frac{x}{y} = -\frac{1}{a}\frac{1 + bx + cy}{x}.$$

f hat höchstens für $x = y = 0$ eine Polstelle, also in P. Andererseits ist x uniformisierend in P, also sieht man aus der zweiten Darstellung $v_P(f) = -1$.
Im Unendlichen: Wir haben projektiv $x_0x_2 + ax_1^2 + bx_1x_2 + cx_2^2 = 0$, also im Unendlichen die Punkte mit $x_0 = 0$ und $ax_1^2 + bx_2x_2 + cx_2^2 = 0$. Für sie gilt $x_2 \neq 0$. Wir führen also affine Koordinaten u, v mit $(u : v : 1) = (x_0 : x_1 : x_2) = (1 : x : y) = (\frac{1}{x} : \frac{x}{y} : 1)$ ein. Also ist $f = v$, insbesondere hat f keine Polstelle im Unendlichen.
Also hat f genau eine Polstelle, nämlich in P, woraus sofort

$$\mathcal{L}(P) = \overline{K} + \overline{K}\frac{x}{y}$$

folgt.

Konstruktion von rationalen Abbildungen: Sei D ein Divisor auf C mit $\ell(D) \geq 2$. Sei $f_0, \dots, f_r$ eine $\overline{K}$-Basis von $\mathcal{L}(D)$. Dann definieren wir $\phi_D : C \to \mathbf{P}^r$ durch

$$\phi_D = (f_0 : \cdots : f_r).$$

(Wählt man eine andere Basis von $\mathcal{L}(D)$, so bedeutet dies einen Basiswechsel in $\mathbf{P}^r$.)
Gilt $\mathcal{L}(D) = \mathcal{L}(D-P)$ für einen Punkt P, so können wir $D-P$ statt D betrachten. Wir setzen also voraus

$$\mathcal{L}(D-P) \neq \mathcal{L}(D), \text{ d.h. } \ell(D-P) = \ell(D) - 1$$

für alle Punkte P. (Man nennt ein solches D basispunktfrei.)
Sei $P \in C$ und t_P uniformisierend in P. Sei n_P die Multiplizität des Divisors D in P, also $D = n_P P + \dots$. Dann ist $v_P(f_i t_P^{n_P}) \geq 0, = 0$ für mindestens einen Index i und

$$\phi_D(P) = ((f_0 t_P^{n_P})(P) : \cdots : (f_r t_P^{n_P})(P)).$$

Wir untersuchen, wann ϕ_D injektiv ist. Es gilt:

$$\begin{aligned}
\phi_D(P) \neq \phi_D(Q) \quad &\iff \quad \text{es gibt eine Hyperebene } H = \{a_0x_0 + \cdots + a_rx_r = 0\} \text{ mit } \phi_D(P) \in H, \phi_D(Q) \notin H \\
&\iff \quad \text{es gibt } a_0, \dots, a_r \text{ nicht alle 0 mit } (\textstyle\sum a_i f_i t_P^{n_P})(P) = 0, (\sum a_i f_i t_Q^{n_Q})(Q) \neq 0 \\
&\iff \quad \text{es gibt } a_0, \dots, a_r \text{ nicht alle 0 mit } \textstyle\sum a_i f_i \in \mathcal{L}(D-P), \sum a_i f_i \notin \mathcal{L}(D-P-Q) \\
&\iff \quad \mathcal{L}(D-P-Q) \neq \mathcal{L}(D-P) \\
&\iff \quad \ell(D-P-Q) = \ell(D-P) - 1 = \ell(D) - 2
\end{aligned}$$

Damit haben wir folgenden Satz zumindest teilweise bewiesen

SATZ 28. *Genau dann ist ϕ_D eine Einbettung, wenn für alle $P, Q \in C$ gilt:*

$$\ell(D-P-Q) = \ell(D) - 2.$$

In diesem Fall ist $deg(D)$ der Grad von C in $\mathbf{P}^r$ mit $r = \ell(D) - 1$. Man nennt D dann auch sehr ampel.

Noch eine Bemerkung zum Grad von $\phi_D(C)$: Ist $D = n_1P_1 + \cdots + n_rP_r$, so kann man nach Koordinatenwechsel $v_{P_i}(f_0) = -n_i$ annehmen. Damit hat f_0 $n_1 + \cdots + n_r = deg(D)$ Polstellen, also ebensoviele Nullstellen. Die Nullstellen liefern den Schnitt von $\phi_D(C)$ mit der Hyperebene $x_0 = 0$, woraus sich die Behauptung ergibt.

SATZ 29. *Gilt $deg(D) \geq 2g+1$, so ist D sehr ampel, d.h. ϕ_D liefert eine Einbettung $C \simeq \phi_D(C) \subseteq \mathbf{P}^r$.*

Beweis: Wegen $deg(K) = 2g-2$ gilt $deg(K-D) < 0$, also $\ell(K-D) = 0$ und somit $\ell(D) = deg(D)+1-g$. Seien jetzt $P, Q \in C$ beliebig. Dann gilt $deg(D-P-Q) \geq 2g-2 > deg(K)$, also $deg(K-(D-P-Q)) < 0$ und somit $\ell(K-(D-P-Q)) = 0$. Riemann-Roch liefert $\ell(D-P-Q) = deg(D-P-Q)+1-g = deg(D)+1-g-2 = \ell(D)-2$. Mit dem vorangegangenen Satz folgt die Behauptung. ■

Beispiele:

1. $C = \mathbf{P}^1$: Für $n \geq 1$ hat $\mathcal{L}(n\infty)$ als Basis $1, t, t^2, \dots, t^n$. Also ist

$$\phi_{n\infty} = (1 : t : \cdots : t^n).$$

   Das Bid ist die sogenannte rationale Normkurve vom Grad n im $\mathbf{P}^n$:

$$\phi_{n\infty}(\mathbf{P}^1) = \{(t_0^n : t_0^{n-1}t_1 : \cdots : t_1^n) : (t_0 : t_1) \in \mathbf{P}^1\}.$$

2. Die Kurve C mit $y^2 = x^3 - x$ hat Geschlecht 1 und den unendlich fernen Punkt $P = (0:0:1)$. Es ist $v_P(x) = -2, v_P(y) = -3$. Wie sieht ϕ_{4P} aus? $\mathcal{L}(4P)$ hat als Basis $1, x, y, x^2$, also: $\phi_{4P} : C \to \mathbf{P}^3$ mit

$$\phi_{4P} = (1 : x : y : x^2).$$

   Das Bild ist eine Kurve vom Grad 4 in $\mathbf{P}^3$. Verwendet man in $\mathbf{P}^3$ die homogenen Koordinaten z_0, z_1, z_2, z_3, so gelten folgende Gleichungen für das Bild:

$$z_1^2 = x^2 = z_0z_3, \quad z_2^2 = y^2 = x \cdot x^2 - x = z_1z_3 - z_1z_0.$$

   Man kann zeigen, daß diese Gleichungen das Bild beschreiben.

3. Ist C eine Kurve vom Geschlecht 2 und wählt man 5 Punkte $P_1, \ldots, P_5$, so ist $D = P_1 + \cdots + P_5$ sehr ampel. Wegen $deg(D) = 5$ und $\ell(D) = 4$ liefert ϕ_D eine Einbettung von C in $\mathbf{P}^3$ als Kurve vom Grad 5.

KAPITEL 7

Kurven vom Geschlecht 0

Wenn nichts anderes erwähnt wird, bezeichnet C eine irreduzible nichtsinguläre projektive Kurve, die über K definiert ist.

SATZ 30. *Hat C Geschlecht* 0 *und gibt es einen über K-definierten Divisor D vom Grad* 1*, so ist C (über K) isomorph zu $\mathbf{P}^1$. D.h. C besitzt eine über K-definierte Parametrisierung:*

$$C = \{(f_0(t_0,t_1) : f_1(t_0,t_1) : \cdots : f_r(t_0,t_1)) : (t_0 : t_1) \in \mathbf{P}^1\},$$

wo die f_i homogene Polynome gleichen Grades mit Koeffizienten in K sind.

Beweis: Da C Geschlecht 0 hat, gilt $deg(K) = -2$, also $deg(K-D) = -3$ und somit $\ell(K-D) = 0$. Riemann-Roch liefert $\ell(D) = 1+1-0 = 2$. Da D über K definiert ist, gibt es Funktionen $f_0, f_1 \in K(C)$ mit $\mathcal{L}(D) = \overline{K}f_0 + \overline{K}f_1$. Der Morphismus $\phi_D : C \to \mathbf{P}^1$ mit $\phi_D = (f_0 : f_1)$ ist dann über K definiert. Nun ist $deg(D) = 1 \geq 2g+1$. Aus dem letzten Abschnitt wissen, daß dann ϕ_D eine Einbettung liefert, d.h. einen Isomorphismus aufs Bild. Also ist ϕ_D ein über K-definierter Isomorphismus und damit $C \simeq \mathbf{P}^1$, was wir zeigen wollten. ■

FOLGERUNG 11. *Hat C Geschlecht* 0 *und besitzt C einen K-rationalen Punkt, so ist $C \simeq_K \mathbf{P}^1$ und insbesondere $\#C(K) = \infty$.*

Beweis: Ist P ein K-rationaler Punkt, so ist P natürlich auch ein K-rationaler Divisor vom Grad 1, woraus die Behauptung mit dem Satz folgt. ■

Über dem algebraischen Abschluß gibt es natürlich immer Punkte, also folgt (mit $K = \overline{K}$):

FOLGERUNG 12. *Jede Kurve C vom Geschlecht* 0 *ist über $\overline{K}$ isomorph zu $\mathbf{P}^1$. Über algebraisch abgeschlossenem Körper gibt es also bis auf Isomorphie genau eine Kurve vom Geschlecht* 0*, nämlich $\mathbf{P}^1$.*

Da die Picardgruppe über dem algebraischen Abschluß berechnet wird, folgt unmittelbar

FOLGERUNG 13. *Hat C Geschlecht* 0*, so gilt*

$$Pic(C) \simeq \mathbf{Z} \quad \text{und } Pic^0(C) = 0.$$

Nicht jede Kurve vom Geschlecht 0 ist (über K) isomorph zu $\mathbf{P}^1$, wie folgendes Beispiel zeigt:

Beispiel: Sei $C = \{2x_0^2 + 3x_1^2 + 5x_2^2 = 0\} \subseteq \mathbf{P}^2$. Die Kurve C ist über $\mathbf{Q}$ definiert, hat als glatte Quadrik Geschlecht 0, hat keine reellen Punkte, insbesondere $C(\mathbf{Q}) = \emptyset$. Damit kann C auch nicht über $\mathbf{Q}$ isomorph zu $\mathbf{P}^1$ sein.

Die folgenden Sätze geben Situationen an, wo man sofort weiß, daß eine Kurve vom Geschlecht 0 isomorph zu $\mathbf{P}^1$ ist.

SATZ 31. *Ist $C \subseteq \mathbf{P}^n$ eine Kurve ungeraden Grades vom Geschlecht* 0*, so ist C isomorph zu $\mathbf{P}^1$ (über K).*

Beweis: Sei H der Divisor eines Hyperebenenschnitts. Er ist über K definiert und $deg(H) = 2m+1$. Sei K ein über K definierter kanonischer Divisor. Es gilt $deg(K) = -2$. Dann ist $H - mK$ über K definiert mit $deg(H - mK) = 1$, also folgt nach unserem Satz $C \simeq \mathbf{P}^1$. ■

Beispiel: Ist $C \subseteq \mathbf{P}^n$ eine über K definierte Gerade, so ist $C \simeq \mathbf{P}^1$, es gibt also eine Parametrisierung

$$C = \{(a_0u + b_0v : \cdots : a_nu + b_nv) : (u : v) \in \mathbf{P}^1\}$$

mit $a_0, b_0, \ldots, a_n, b_n \in K$.

Satz 32. *Ist $\tilde{C} \subseteq \mathbf{P}^n$ eine irreduzible über K definierte Kurve ungeraden Grades mit nur endlich vielen Singularitäten, so daß die Desingularisierung C Geschlecht 0 hat, so ist $C \simeq \mathbf{P}^1$, also gibt es eine Parametrisierung*

$$\tilde{C} = \{(f_0(t_0,t_1) : f_1(t_0,t_1) : \cdots : f_r(t_0,t_1)) : (t_0 : t_1) \in \mathbf{P}^1\},$$

wo die f_i homogene Polynome gleichen Grades mit Koeffizienten in K sind.

Beweis: Man wähle einen über K definierten Hyperebenenschnitt, der keine Singularität enthält. (K unendlich?) Dies liefert auf C einen Divisor H, der über K definiert ist und ungeraden Grad hat. Die Behauptung folgt mit dem letzten Satz. ■

Beispiel: Ist $f(x_0,x_1,x_2) = 0$ eine irreduzible ebene Kubik mit einer Singularität, so ist die Desingularisierung isomorph zu $\mathbf{P}^1$. Wählt man z.B. die Kurve

$$C = \{-27x_0^2x_1 + 152x_0^3 - 75x_0^2x_2 + 4x_1^3 + 4x_2^3 = 0\},$$

so stellt man fest, daß sie genau in $(2:3:5)$ eine Singularität hat. Substituiert man $x_0 = 1, x_1 = x, x_2 = y$ und $y = \frac{5}{2} + t(x - \frac{3}{2})$ (Geraden durch die Singularität), so spaltet der Faktor $(2x-3)^2$ ab und aus dem Rest erhält man eine Parametrisierung:

$$x_0 = 2t^3 + 2, \quad x_1 = 3t^3 - 15t^2 - 6, \quad x_2 = -10t^3 - 9t + 5.$$

Frage: Wie kann man sich Kurven vom Geschlecht 0 vorstellen?

Diese Frage beantwortet folgender Satz:

Satz 33. *Jede Kurve C vom Geschlecht 0 ist über K isomorph zu einem (glatten) ebenen Kegelschnitt, d.h. zu einer (glatten) Kurve*

$$\{a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = 0\}$$

mit $a_0, a_1, a_2, a_3, a_4, a_5$ in K.

Beweis: Wähle $f \in K(C)$ mit $df \neq 0$. Dann ist der kanonische Divisor $K = (df)$ über K definiert. Es gilt

$$deg(-K) = 2 \text{ und } \ell(-K) = 2 + 1 - 0 + \ell(2K) = 3,$$

es gibt also $f_0, f_1, f_2 \in K(C)$, die eine Basis von $\mathcal{L}(-K)$ bilden. Wegen $deg(-K) \geq 2g+1$ ist $-K$ sehr ampel, d.h. $\phi_{-K} : C \to \mathbf{P}^2$ mit $\phi_{-K} = (f_0 : f_1 : f_2)$ ist eine Einbettung. Also $C \simeq_K \phi_{-K}(C) \subseteq \mathbf{P}^2$ und $\phi_{-K}(C)$ hat Grad 2. Außerdem ist ϕ_{-K} über K definiert. Damit folgt die Behauptung. ■

Eine kleine Anmerkung zur Glattheit von Kegelschnitten:

Satz 34. *Für einen ebenen Kegelschnitt C mit der Gleichung*

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = 0$$

sind äquivalent:

1. *C ist absolut irreduzibel,*
2. *C ist glatt,*
3. $4a_0a_3a_5 + a_1a_2a_4 - a_2^2a_3 - a_0a_4^2 - a_1^2a_5 \neq 0$.

Beweisskizze: Zunächst zeigt man, daß Glattheit und Irreduzibilität für ebene Quadriken das gleiche ist. Weiter gilt

$$\begin{pmatrix} \frac{\partial f}{\partial x_0} \\ \frac{\partial f}{\partial x_1} \\ \frac{\partial f}{\partial x_2} \end{pmatrix} = \begin{pmatrix} 2a_0 & a_1 & a_2 \\ a_1 & 2a_3 & a_4 \\ a_2 & a_4 & 2a_5 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}.$$

Mit

$$D = 4a_0a_3a_5 + a_1a_2a_4 - a_2^2a_3 - a_0a_4^2 - a_1^2a_5$$

ist die Determinante der 3×3-Matrix $2D$.
$char(K) \neq 2$: Folgt unmittelbar.
$char(K) = 2$: Ist $a_1 = a_2 = a_4 = 0$, so ist f Quadrat und $D = 0$. Sei also $(a_1, a_2, a_4) \neq 0$. Dann gilt $\{f_0 = f_1 = f_2\} = \{(a_4 : a_2 : a_1)\}$ und $f(a_4, a_2, a_1) = D$, woraus sofort die Behauptung folgt. ■

Die nächste Frage, die sich stellt, ist:

Frage: Wann sind zwei über K definierte ebene Kegelschnitte über K isomorph?

Eine Antwort gibt der folgende Satz:

SATZ 35. *Zwei über K definierte (nichtsinguläre) Kegelschnitte sind genau dann isomorph über K, wenn sie über K projektiv äquivalent sind, d.h. durch Koordinatenwechsel über K auseinanderhervorgehen.*

Beweis: Projektiv äquivalente Kegelschnitte sind natürlich auch isomorph, also müssen wir nur die Umkehrung zeigen. Seien C_1 und C_2 zwei ebene Kegelschnitte und $\psi : C_1 \to C_2$ ein über K definierter Isomorphismus.

- $H_i = (x_0)$ ist ein über K definierter Geradenschnitt von C_i. Er hat Grad 2, also $\ell(H_i) = 3$. Nach Riemann-Roch gilt
$$\mathcal{L}(H_i) = \overline{K} + \overline{K}\frac{x_1}{x_0} + \overline{K}\frac{x_2}{x_0},$$
also $\phi_{H_i} = (1 : \frac{x_1}{x_0} : \frac{x_2}{x_0}) = (x_0 : x_1 : x_2)$, d.h. $\phi_{H_i} = id_{C_i}$.
- $\psi^* H_2$ ist ein über K definierter Divisor vom Grad 2, wegen $Pic^0(C_1) = 0$ sind $\psi^* H_2$ und H_1 linear äquivalent, es gibt also eine Funktion $f \in K(C)$ mit $\psi^* H_2 = H_1 + (f)$.
- Es gilt
$$H_1 + (f\psi^* \frac{x_i}{x_0}) = \psi^* H_2 + \psi^*(\frac{x_i}{x_0}) = \psi^*(H_2 + (\frac{x_i}{x_0})) \geq 0,$$
also $f\psi^* \frac{x_i}{x_0} \in \mathcal{L}(H_1)$. Wegen $f\psi^* \frac{x_i}{x_0} \in K(C_1)$ gibt es also $a_{ij} \in K$ mit $f\psi^* \frac{x_i}{x_0} = \sum_j a_{ij} \frac{x_j}{x_0}$.
- Nun gilt für $P \in C_1$ mit Wahl einer geeigneten Funktion $g \in \overline{K}(C_2)$:
$$\begin{aligned}
\psi(p_0 : p_1 : p_2) &= \psi(P) = (x_0(\psi(P)) : x_1(\psi(P)) : x_2(\psi(P))) = \\
&= (g(\psi(P)) : (g\frac{x_1}{x_0})(\psi(P)) : (g\frac{x_2}{x_0})(\psi(P))) = \\
&= (\psi^*(g)(P)) : (\psi^*(g\frac{x_1}{x_0})(P) : (\psi^*(g\frac{x_2}{x_0})(P)) = \\
&= \psi^*(g) \begin{pmatrix} \psi^* \frac{x_0}{x_0} \\ \psi^* \frac{x_1}{x_0} \\ \psi^* \frac{x_2}{x_0} \end{pmatrix} (P) = \\
&= \psi^*(g) \cdot f \cdot (a_{ij}) \begin{pmatrix} \frac{x_0}{x_0} \\ \frac{x_1}{x_0} \\ \frac{x_2}{x_0} \end{pmatrix} (P) = \\
&= (a_{ij}) \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} (P) = \\
&= (\tilde{a_{ij}})(p_0 : p_1 : p_2),
\end{aligned}$$
wo $(\tilde{a_{ij}})$ die entsprechend angegebene Operation bedeutet. ■

Die Klassifikation der Kegelschnitte ist ein eigenes Thema, das stark vom Grundkörper abhängt. Wir wollen uns zunächst auf endliche Körper und $\mathbf{Q}$ beschränken und dann nur untersuchen, wann ein Kegelschnitt isomorph zu $\mathbf{P}^1$ ist, d.h. einen K-rationalen Punkt besitzt.

Bemerkung: Ist die Charakteristik von $K \neq 2$, so lernt man schon in der Linearen Algebra, daß man jeden Kegelschnitt durch quadratische Ergänzungen diagonalisieren kann, d.h. $a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = 0$ läßt sich immer auf die Gestalt
$$b_0x_0^2 + b_1x_1^2 + b_2x_2^2 = 0$$
transformieren.

Beispiel: Wir betrachten über $\mathbf{Q}$ die Quadrik
$$g = 431x_0^2 + 865x_0x_1 + 216x_0x_2 + 431x_1^2 + 216x_1x_2 + 36x_2^2 = 0.$$

Macht man den Ansatz $x_0 = y_0 + ay_1 + by_2, x_1 = y_1 + cy_2, x_2 = y_2$, setzt ein, bestimmt a, b, c so, daß die Koeffizienten bei y_0y_1, y_0y_2, y_1y_2 verschwinden, so erhält man

$$x_0 = y_0 - 865/862y_1 - 216/1727y_2, x_1 = y_1 - 216/1727y_2, x_2 = y_2$$

und

$$\tilde{g} = 431y_0^2 - \frac{5181}{1724}y_1^2 + \frac{15516}{1727}y_2^2.$$

Quadriken über endlichen Körpern

Sei $\mathbf{F}_q$ der Körper mit q Elementen, $q = p^m$. Die Polynome x^q und x sind als Funktionen auf $\mathbf{F}_q$ identisch, nicht jedoch als Polynome.

LEMMA 8. *Sind $f, g \in \mathbf{F}_q[x_1, \ldots, x_n]$ Polynome mit $grad_{x_i} f, grad_{x_i} g \leq q-1$ für $i = 1, \ldots, n$, so gilt:*

$$f|_{\mathbf{F}_q^n} = g|_{\mathbf{F}_q^n} \quad \Rightarrow \quad f = g.$$

Beweis: Indem wir $f - g$ betrachten, reicht es, folgendes zu zeigen: $f|_{\mathbf{F}_q^n} = 0 \Rightarrow f = 0$. Wir beweisen dies durch Induktion nach n.
$n = 1$: Das Polynom $f = a_0 + a_1x + \cdots + a_{q-1}x^{q-1}$ hat mindestens q Nullstellen, was nur für $f = 0$ passieren kann.
$n \geq 2$: Wir schreiben

$$f(x_1, \ldots, x_n) = g_0(x_1, \ldots, x_{n-1}) + g_1(x_1, \ldots, x_{n-1})x_n + \cdots + g_{q-1}(x_1, \ldots, x_{n-1})x_n^{q-1}$$

Ist $(a_1, \ldots, a_{n-1}) \in \mathbf{F}_q^{n-1}$, so ist $f(a_1, \ldots, a_{n-1}, x_n)$ als Funktion 0 auf $\mathbf{F}_q$. Nach dem Fall $n = 1$ folgt

$$g_i(a_1, \ldots, a_{n-1}) = 0 \text{ für } i = 0, \ldots, q-1.$$

Da $(a_1, \ldots, a_{n-1})$ beliebig war, folgt nach Induktionsannahme sofort $g_i = 0$, also $f = 0$ als Polynom. ■

SATZ 36. *Ist $f(x_1, \ldots, x_n) \in \mathbf{F}_q[x_1, \ldots, x_n]$ vom Grad $d < n$ und $f(a_1, \ldots, a_n) = 0$ für ein $(a_1, \ldots, a_n) \in \mathbf{F}_q^n$, so hat f mindestens noch eine zweite Nullstelle.*

Beweis: Wir nehmen an, $(a_1, \ldots, a_n)$ ist die einzige Nullstelle von f in $\mathbf{F}_q^n$. Dann gilt für das Polynom auf $\mathbf{F}_q^n$:

$$g(x_1, \ldots, x_n) = 1 - f(x_1, \ldots, x_n)^{q-1} = \left\{ \begin{array}{lll} 0 & \text{für} & (x_1, \ldots, x_n) \neq (a_1, \ldots, a_n) \\ 1 & \text{für} & (x_1, \ldots, x_n) = (a_1, \ldots, a_n) \end{array} \right\},$$

da für $a \in \mathbf{F}_q \setminus \{0\}$ gilt $a^{q-1} = 1$. Die gleiche Polynomfunktion auf $\mathbf{F}_q^n$ liefert auch

$$h(x_1, \ldots, x_n) = \prod_{i=1}^{n} (1 - (x_i - a_i)^{q-1}).$$

Es gilt $grad_{x_i} h = q - 1$. Sei $\tilde{g}$ das Polynom, das aus $g(x_1, \ldots, x_n)$ entsteht, wenn man soweit möglich x_i^q durch x_i ersetzt. Dann gilt auch $grad_{x_i} \tilde{g} \leq q - 1$ und natürlich weiterhin $\tilde{g}|_{\mathbf{F}_q^n} = h_{\mathbf{F}_q^n}$. Nach dem Lemma gilt also $\tilde{g} = h$. Nun gilt für den Totalgrad

$$n(q-1) = grad(h) = grad(\tilde{g}) \leq grad(g) \leq d(q-1),$$

was $n \leq d$, also einen Widerspruch zur Voraussetzung liefert. Damit folgt die Behauptung. ■

Da ein homogenes Polynom natürlich immer die triviale Nullstelle hat, folgt sofort

SATZ 37 (Chevalley). *Ist $f(x_1, \ldots, x_n) \in \mathbf{F}_q[x_1, \ldots, x_n]$ ein homogenes Polynom vom Grad $d < n$, so besitzt $f = 0$ eine nichttriviale Nullstelle in $\mathbf{F}_q^n$.*

FOLGERUNG 14. *Ist $f(x_0, x_1, x_2) \in \mathbf{F}_q[x_0, x_1, x_2]$ ein homogenes quadratisches Polynom, so besitzt $f = 0$ eine nichttriviale Nullstelle in $\mathbf{F}_q^3$.*

Jede über $\mathbf{F}_q$ definierte Quadrik in $\mathbf{P}^2$ besitzt also einen $\mathbf{F}_q$-rationalen Punkt, woraus sich sofort ergibt:

SATZ 38. *Ist C eine Kurve vom Geschlecht 0, die über $\mathbf{F}_q$ definiert ist, so ist C über $\mathbf{F}_q$ isomorph zu $\mathbf{P}^1$.*

Wir wollen noch sehen, daß sich der Satz von Chevalley nicht verschärfen läßt:

Beispiel: Sei $d \geq n$ gegeben. $\mathbf{F}_{q^d}$ ist eine galoissche Körpererweiterung vom $\mathbf{F}_q$. Sei $\alpha_1, \ldots, \alpha_d$ eine $\mathbf{F}_q$-Basis von $\mathbf{F}_{q^d}$ und $G = \{\sigma_1, \ldots, \sigma_d\}$ die Galoisgruppe von $\mathbf{F}_{q^d}$ über $\mathbf{F}_q$. Wegen $n \leq d$ kann man definieren

$$f(x_1, \ldots, x_n) = \prod_{i=1}^{d} (\sigma_i \alpha_1 x_1 + \cdots + \sigma_i \alpha_n x_n).$$

f ist homogen vom Grad d in n Veränderlichen. Zunächst hat f Koeffizienten in $\mathbf{F}_{q^d}$. Es gilt aber $\sigma f = f$ für alle $\sigma \in G$, also hat f schon Koeffizienten in $\mathbf{F}_q$.
Ist $(a_1, \ldots, a_n) \in \mathbf{F}_q^n \setminus \{0\}$, so ist $a_1\alpha_1 + \cdots + a_n\alpha_n \neq 0$, also auch $f(a_1, \ldots, a_n) \neq 0$. D.h. f hat nur die triviale Nullstelle in $\mathbf{F}_q^n$. Damit sehen wir, daß sich der Satz von Chevalley nicht verschärfen läßt.

Ebene Quadriken über Q

Wir betrachten eine nichtsinguläre ebene Quadrik

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = 0$$

mit $a_i \in \mathbf{Q}$ und wollen untersuchen, wann $f = 0$ rationale Punkte besitzt.

Reduktionsschritte:

1. Zunächst bringen wir die Quadrik durch quadratische Ergänzungen auf die Diagonalgestalt
$$f = b_0x_0^2 + b_1x_1^2 + b_2x_2^2 = 0.$$
2. Damit rationale Punkte existieren können, müssen b_0, b_1, b_2 unterschiedliches Vorzeichen haben. Indem wir Koordinaten vertauschen und eventuell mit -1 multiplizieren, können wir die Gleichung in der Form
$$f = ax^2 + by^2 - cz^2 = 0 \text{ mit } a, b, c \in \mathbf{N}$$
schreiben.
3. Nach Division durch $ggT(a, b, c)$ können wir $ggT(a, b, c) = 1$ annehmen.
4. Ist a nicht quadratfrei, d.h. $a = d^2 \cdot \tilde{a}$, so ist $ax^2 = \tilde{a}(dx)^2$, nach Koordinatenwechsel $\tilde{x} = dx$ können wir also erreichen, daß a quadratfrei ist. Analog können wir b und c als quadratfrei voraussetzen.
5. Gibt es eine Primzahl p mit $a = pa_1, b = pb_1$, so ist
$$p(ax^2 + by^2 - cz^2) = a_1(px)^2 + b_1(py)^2 - pcz^2.$$
Nach Koordinatenwechsel $x_1 = px, y_1 = py$ teilt p weder a_1 noch a_2. Wendet man diesen Reduktionsprozeß an, auch auf a, c und b, c, so kann man erreichen, daß a, b, c paarweise teilerfremd sind.

Wir können uns also auf Gleichungen der Form $f = ax^2 + by^2 - cz^2 = 0$ mit $a, b, c \in \mathbf{N}$, a, b, c paarweise teilerfremd und a, b, c quadratfrei beschränken.

Notwendige Bedingung für die Existenz einer rationalen Lösung: Sei (x_0, y_0, z_0) eine Lösung. O.E. können wir $x_0, y_0, z_0 \in \mathbf{Z}$ mit $ggT(x_0, y_0, z_0) = 1$ annehmen.
Ist p eine ungerade Primzahl mit $p|c$, dann teilt p weder a noch b. Außerdem teilt p auch nicht x_0 und y_0. (Würde gelten $p|x_0$, so folgte $p|y_0$, also $p^2|ax_0^2 + by_0^2$ und somit $p^2|cz_0^2$, was $p|z_0$ lieferte. Analog für $p|y_0$.) Damit gilt modulo p:

$$ax_0^2 + by_0^2 \equiv 0 \Rightarrow -abx_0^2 \equiv (by_0)^2 \Rightarrow -ab \equiv (\frac{by_0}{x_0})^2 \bmod p,$$

d.h. $-ab$ ist ein Quadrat modulo p, das Legendresymbol gilt daher $\left(\frac{-ab}{p}\right) = 1$.
Auf die gleiche Weise erhält man noch folgende zwei Bedingungen:

$$p|a, p \text{ ungerade Primzahl} \quad \Rightarrow \quad \left(\frac{bc}{p}\right) = 1,$$

$$p|b, p \text{ ungerade Primzahl} \quad \Rightarrow \quad \left(\frac{ac}{p}\right) = 1.$$

Damit können wir jetzt folgenden Satz beweisen, der auf Legendre zurückgeht:

Satz 39. *Seien $a, b, c \in \mathbf{N}$ paarweise teilerfremd und quadratfrei. Dann hat die Quadrik $C = \{ax^2 + by^2 - cz^2 = 0\}$ genau dann $\mathbf{Q}$-rationale Punkte, wenn gilt:*

$$\left(\frac{-ab}{p}\right) = 1 \qquad \text{für alle ungeraden Primzahlen } p \text{ mit } p|c,$$
$$\left(\frac{ac}{p}\right) = 1 \qquad \text{für alle ungeraden Primzahlen } p \text{ mit } p|b,$$
$$\left(\frac{bc}{p}\right) = 1 \qquad \text{für alle ungeraden Primzahlen } p \text{ mit } p|a.$$

Beweis: Die Notwendigkeit der Bedingung haben wir bereits gesehen. Wir setzen jetzt umgekehrt die Bedingungen voraus und wollen eine rationale Lösung konstruieren.

1. Ist p eine ungerade Primzahl mit $p|c$, so ist $\left(\frac{-ab}{p}\right) = 1$, also gibt es $u \in \mathbf{Z}$ mit $-ab \equiv u^2 \bmod p$ und somit
$$ax^2 + by^2 - cz^2 \equiv a(x^2 - \frac{u^2}{a^2}y^2) = a(x - \frac{u}{a}y)(x + \frac{u}{a}y) \bmod p.$$
Es gibt also Linearformen $g_p(x, y, z), h_p(x, y, z)$ (mit Koeffizienten in $\mathbf{Z}$) mit
$$ax^2 + by^2 - cz^2 \equiv g_p(x, y, z)h_p(x, y, z) \bmod p.$$
2. In gleicher Weise findet man für jede ungerade Primzahl p mit $p|abc$ Linearformen $g_p(x, y, z), h_p(x, y, z)$ (mit Koeffizienten in $\mathbf{Z}$) mit
$$ax^2 + by^2 - cz^2 \equiv g_p(x, y, z)h_p(x, y, z) \bmod p.$$
3. Gilt $2|abc$, so setze man $g_2(x, y, z) = h_2(x, y, z) = ax + by + cz$. Man hat schließlich für jede Primzahl p mit $p|abc$ die Beziehung
$$ax^2 + by^2 - cz^2 \equiv g_p(x, y, z)h_p(x, y, z) \bmod p.$$
4. Mit dem chinesischen Restsatz findet man Linearformen $g(x, y, z), h(x, y, z)$ (mit Koeffizienten in $\mathbf{Z}$) mit
$$g(x, y, z) \equiv g_p(x, y, z) \bmod p, \quad h(x, y, z) \equiv h_p(x, y, z) \bmod p,$$
für jede Primzahl p mit $p|abc$.
5. Es folgt jetzt sofort
$$ax^2 + by^2 - cz^2 \equiv g(x, y, z)h(x, y, z) \bmod abc.$$
6. Wir betrachten jetzt die Menge
$$M = \{(x, y, z) \in \mathbf{Z}^3 : 0 \le x < \sqrt{bc}, 0 \le y < \sqrt{ac}, 0 \le z < \sqrt{ab}\}.$$
Ist $\sqrt{bc}$ eine natürliche Zahl, so ist $b = c = 1$ und wir sind fertig. Also können wir $\sqrt{bc}$ irrational annehmen, es gilt dann
$$\#M \ge (1 + [\sqrt{bc}])\sqrt{ac}\sqrt{ab} > \sqrt{bc}\sqrt{ac}\sqrt{ab} = abc.$$
$$g \bmod abc : M \to \mathbf{Z}/(abc)$$
ist daher nicht injektiv, es gibt also zwei verschiedene $(x_1, y_1, z_1), (x_2, y_2, z_2) \in M$ mit $g(x_1, y_1, z_1) \equiv g(x_2, y_2, z_2) \bmod abc$. Setzt man $x_0 = x_1 - x_2, y_0 = y_1 - y_2, z_0 = z_1 - z_2$, so ist $g(x_0, y_0, z_0) \equiv 0 \bmod abc$, $(x_0, y_0, z_0) \ne 0$ und
$$|x_0| < \sqrt{bc}, \quad |y_0| < \sqrt{ac}, \quad |z_0| < \sqrt{ab}.$$
7. Es folgt sofort $f(x_0, y_0, z_0) \equiv 0 \bmod abc$. Wegen
$$0 \le ax_0^2, by_0^2, cz_0^2 < abc$$
folgt
$$-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc.$$
Daher ist
$$ax_0^2 + by_0^2 - cz_0^2 \in \{0, abc\}.$$

Ist $ax_0^2 + by_0^2 - cz_0^2 = 0$ sind wir fertig, ist $ax_0^2 + by_0^2 - cz_0^2 = abc$, so gilt mit dem nachfolgenden Lemma

$$a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 - c(z_0^2 + ab)^2 = 0,$$

also haben wir auch eine Lösung. ■

LEMMA 9. *Die Gleichung $ax_0^2 + by_0^2 - cz_0^2 = abc$ liefert die Gleichungen*

$$a(x_0z_0+by_0)^2+b(y_0z_0-ax_0)^2-c(z_0^2+ab)^2=0 \quad \text{und} \quad a(x_0z_0-by_0)^2+b(y_0z_0+ax_0)^2-c(z_0^2+ab)^2=0.$$

Beweis: Dies kann man natürlich einfach nachrechnen. Wie kommt dies zustande? $f = ax^2+by^2-cz^2 = 0$ ist ein ebener Kegelschnitt. Vom Punkt $(x_0 : y_0 : z_0)$ aus wird es i.a. zwei Tangenten an $f = 0$ geben. Die Schnittpunkte mit dem Kegelschnitt sind obige Punkte. ■

Beispiel: Wir betrachten $f = ax^2 + by^2 - cz^2$ mit

$$a = 595 = 5 \cdot 7 \cdot 17, \quad b = 929, \quad c = 129 = 3 \cdot 43.$$

Dann erfüllt f die notwendigen Bedingungen. Man erhält

$$\begin{aligned} f &\equiv (x+y)(x+2y) \bmod 3 \\ f &\equiv (4y+z)(y+z) \bmod 5 \\ f &\equiv (y+4z)(5y+z) \bmod 7 \\ f &\equiv (12y+7z)(8y+z) \bmod 17 \\ f &\equiv (36x+15y)(x+39y) \bmod 43 \\ f &\equiv (58x+800z)(699x+z) \bmod 929 \end{aligned}$$

Die linken Faktoren seien $g_p(x,y,z)$, die rechten $h_p(x,y,z)$, der chinesische Restsatz liefert dann

$$g = 1535695x + 6141619y + 71305266z, \quad h = 37025065x + 69609041y + 7185816z.$$

Sucht man im Bereich $|x| \le 346, |y| \le 277, |z| \le 743$, so erhält man viele Lösungen der Kongruenz $g(x,y,z) \equiv 0 \bmod abc$.
Wir beschränken uns auf Lösungen mit $ggT(x,y,z) = 1$ und $x \ge 0$. f kann den Wert 0 oder abc haben. Nur für $(4,-1,9)$ war $f = 0$.
Daneben gab es 74 Fälle mit $f = abc$, z.B. $(53, 277, -113)$.

Beispiel: Wir betrachten $f = ax^2 + by^2 - cz^2$ mit $a = 43, b = 131, c = 462 = 2 \cdot 3 \cdot 7 \cdot 11$. Wir berechnen

$$\left(\frac{-ab}{3}\right) = \left(\frac{-43 \cdot 131}{3}\right) = \left(\frac{-2}{3}\right) = 1, \left(\frac{-43 \cdot 131}{7}\right) = \left(\frac{2}{7}\right) = 1, \left(\frac{-43 \cdot 131}{11}\right) = \left(\frac{10}{11}\right) = \left(\frac{-1}{11}\right) = -1,$$

also besitzt $f = 0$ keine rationalen Punkte.

Beispiel: Wir betrachten nochmals unser Beispiel

$$g = 431x_0^2 + 865x_0x_1 + 216x_0x_2 + 431x_1^2 + 216x_1x_2 + 36x_2^2 = 0.$$

Durch die Transformation

$$x_0 = y_0 - 865/862y_1 - 216/1727y_2, x_1 = y_1 - 216/1727y_2, x_2 = y_2$$

erhält man

$$\begin{aligned} g &= 431y_0^2 - \frac{5181}{1724}y_1^2 + \frac{15516}{1727}y_2^2 = \\ &= \frac{1}{2977348}[1283236988y_0^2 + 26749584y_2^2 - 8947587y_1^2] = \\ &= \frac{1}{2977348}[2^2 \cdot 11 \cdot 157 \cdot 431^2y_0^2 + 2^4 \cdot 3^2 \cdot 431^2y_2^2 - 3 \cdot 11^2 \cdot 157^2y_1^2] = \\ &= \frac{1}{2977348}[11 \cdot 157(2 \cdot 431y_0)^2 + (2^2 \cdot 3 \cdot 431y_2)^2 - 3 \cdot (11 \cdot 157y_1)^2] \end{aligned}$$

Substituieren wir

$$y_0 = \frac{1}{2 \cdot 431}z_0, \quad y_2 = \frac{1}{4 \cdot 3 \cdot 431}z_1, \quad y_1 = \frac{1}{11 \cdot 157}z_2,$$

so ist also bis auf eine Konstante

$$g \sim 11 \cdot 157 z_0^2 + z_1^2 - 3z_2^2.$$

Wir haben also

$$a = 11 \cdot 157, \quad b = 1, \quad c = 3.$$

Wir haben nur drei Lösungsbedingungen:

$$\left(\frac{-11 \cdot 157}{3}\right), \quad \left(\frac{3}{11}\right), \quad \left(\frac{157}{11}\right)$$

müssen 1 sein. Sie sind es auch. Also existiert eine Lösung. In der folgenden Tabelle sind jeweils die kleinsten Lösungen in x- und z-Koordinaten aufgeführt.

$(x_0 : x_1 : x_2)$	$(z_0 : z_1 : z_1)$
$(114414 : -123912 : -1727)$	$(1 : 1 : 24)$
$(66 : -72 : 1)$	$(1 : -1 : 24)$
$(66 : -72 : 35)$	$(181 : 15085 : -9732)$
$(72 : -66 : -35)$	$(1 : 70 : 47)$
$(72 : -66 : -1)$	$(793 : -862 : -19033)$

Wir können jetzt also effektiv entscheiden, ob eine ebene Quadrik, die über $\mathbf{Q}$ definiert ist, rationale Punkte besitzt.

Frage: Gibt es einen guten Algorithmus um Punkte explizit zu finden, falls welche existieren?

Immerhin gibt es Abschätzungen für die kleinste Lösung, die wir ohne Beweis angeben:

SATZ 40. *Ist $ax^2 + by^2 - cz^2 = 0$ mit $a, b, c \in \mathbf{N}$ nichttrivial lösbar, so gibt es eine Lösung $(x_0 : y_0 : z_0)$ mit*

$$|x_0| \leq \sqrt{bc}, \quad |y_0| \leq \sqrt{ac}, \quad |z_0| \leq \sqrt{ab}.$$

Wir wollen allgemein einen Größenbegriff für Punkte des $\mathbf{P}^n(\mathbf{Q})$ einführen: Ist $P \in \mathbf{P}^n(\mathbf{Q})$, so kann man schreiben $P = (a_0 : \cdots : a_n)$ mit $a_i \in \mathbf{Q}$. Da die a_i's nur bis auf einen gemeinsamen Faktor bestimmt sind, kann man $a_i \in \mathbf{Z}$ und $ggT(a_0, \ldots, a_n) = 1$ erreichen. Mit dieser Bedingung sind die a_i's bis aufs Vorzeichen bestimmt. Wir definieren

DEFINITION 36. *Die Höhe eines Punktes $P \in \mathbf{P}^n(\mathbf{Q})$ wird definiert durch*

$$H(P) = \max(|a_0|, \ldots, |a_n|),$$

falls $P = (a_0 : \cdots : a_n)$ mit $a_i \in \mathbf{Z}$ und $ggT(a_0, \ldots, a_n) = 1$.

Eine ebene Quadrik über $\mathbf{Q}$ hat die Gestalt $C = \{a_0 x_0^2 + \cdots + a_5 x_2^2 = 0\}$ mit $a_i \in \mathbf{Q}$. Die Kurve C ist eindeutig bestimmt durch $(a_0 : \cdots : a_5) \in \mathbf{P}^5(\mathbf{Q})$. Daher kann man definieren

$$H(C) = H((a_0 : \cdots : a_5)).$$

Damit können wir in der zweiten Abschätzung noch weiter wie folgt abschätzen:

SATZ 41. *Ist $C \subseteq \mathbf{P}^2$ eine über $\mathbf{Q}$ definierte Quadrik mit $C(\mathbf{Q}) \neq \emptyset$, so gibt es einen Punkt $P \in C(\mathbf{Q})$ mit*

$$H(P) \leq 7H(C).$$

Zum Beweis brauchen wir einen Satz aus der diophantischen Approximation, den wir ohne Beweis angeben:

SATZ 42 (Minkowski's Linearformensatz). *Sei $(\alpha_{ij})_{i,j=1\ldots n}$ eine reelle Matrix mit Determinante ± 1. Seien $A_1, \ldots, A_n$ positive reelle Zahlen mit $A_1 \ldots A_n = 1$. Dann gibt es einen nichttrivialen Gitterpunkt $(x_1, \ldots, x_n) \in \mathbf{Z}^n \setminus \{0\}$ mit*

$$|\alpha_{i1} x_1 + \cdots + \alpha_{in} x_n| < A_i \text{ für } 1 \leq i \leq n-1 \text{ und } |\alpha_{n1} x_1 + \cdots + \alpha_{nn} x_n| \leq A_n.$$

Beispiele:

1. Wählt man (α_{ij}) die Einheitsmatrix und $A_i = 1$, so hat man die Ungleichungen
$$|x_1| < 1, \dots, |x_{n-1}| < 1, |x_n| \leq 1.$$
Nichttriviale Gitterpunkte sind $(0, \dots, 0, \pm 1)$. Man sieht hieran auch, daß nicht lauter $<$-Zeichen möglich sind.
2. Seien α_1, α_2 reelle Zahlen, $m \in \mathbf{N}, m \geq 2$. Wir betrachten die Ungleichungen
$$|x_0| < m, \quad |x_1 - \alpha_1 x_0| \leq \frac{1}{\sqrt{m}}, \quad |x_2 - \alpha_2 x_0| \leq \frac{1}{\sqrt{m}}.$$
Die Voraussetzungen des Satzes sind erfüllt, also gibt es einen nichttrivialen Gitterpunkt (x_0, x_1, x_2), der die Ungleichungen erfüllt.
3. Zur Übung beweise man eine Aussage wie in 2. mit dem Dirichletschen Schubfachprinzip; die Abschätzungen können etwas schlechter sein.

Beweis des Satzes:

1. Wir schreiben $C = \{f = 0\}$ mit
$$f = a_0 x_0^2 + a_1 x_0 x_1 + a_2 x_0 x_2 + a_3 x_1^2 + a_4 x_1 x_2 + a_5 x_2^2,$$
$a_0, \dots, a_5 \in \mathbf{Z}$ und $ggT(a_0, \dots, a_5) = 1$. Sei $P = (p_0 : p_1 : p_2) \in C(\mathbf{Q})$ ein Punkt minimaler Höhe, wo o.E. $p_0, p_1, p_2 \in \mathbf{Z}$, $ggT(p_0, p_1, p_2) = 1$ und $p_0 = \max(|p_0|, |p_1|, |p_2|)$ ist.
2. Wir wählen einen Punkt $Q = (q_0 : q_1 : q_2) \in \mathbf{P}^2(\mathbf{Q})$ mit $Q \notin C$ und o.E. $q_0, q_1, q_2 \in \mathbf{Z}$. Die Punkte der Verbindungsgeraden zwischen P und Q lassen sich wie folgt parametrisieren:
$$x_0 = u p_0 + v q_0, \quad x_1 = u p_1 + v q_1, \quad x_2 = u p_2 + v q_2.$$
Es gilt dann
$$f(up_0 + vq_0, up_1 + vq_1, up_2 + vq_2) = v(Vu - Uv)$$
mit
$$\begin{aligned} U &= a_0 q_0^2 + a_1 q_0 q_1 + a_2 q_0 q_2 + a_3 q_1^2 + a_4 q_1 q_2 + a_5 q_2^2, \\ -V &= a_0 \cdot 2p_0 q_0 + a_1(p_0 q_1 + p_1 q_0) + a_2(p_0 q_2 + p_2 q_0) + a_3 \cdot 2p_1 q_1 + a_4(p_1 q_2 + p_2 q_1) + a_5 \cdot 2p_2 q_2. \end{aligned}$$
Wegen $Q \notin C$ ist $U \neq 0$.
3. Definieren wir jetzt
$$r_0 = U p_0 + V q_0, \quad r_1 = U p_1 + V q_1, \quad r_2 = U p_2 + V q_2,$$
dann gilt $r_i \in \mathbf{Z}$, $(r_0, r_1, r_2) \neq 0$ wegen $P \neq Q$ und $R = (r_0 : r_1 : r_2) \in C(\mathbf{Q})$.
4. Wir versuchen Q so zu finden, daß R möglichst kleine Höhe hat. Wir machen den Ansatz
$$q_0 = \lambda p_0 + \delta_0, \quad q_1 = \lambda p_1 + \delta_1, \quad q_2 = \lambda p_1 + \delta_2.$$
Dann erhält man mit $U = U - \lambda^2 f(p_0, p_1, p_2)$ und $V = V + 2\lambda f(p_0, p_1, p_2)$:
$$\begin{aligned} U &= a_0 \delta_0^2 + a_1 \delta_0 \delta_1 + \dots \\ &\quad + \lambda(a_0 \cdot 2p_0 \delta_0 + a_1(p_0 \delta_1 + p_1 \delta_0) + \dots \\ -V &= a_0 \cdot 2p_0 \delta_0 + a_1(p_0 \delta_1 + p_1 \delta_0) + \dots \end{aligned}$$
und
$$\begin{aligned} r_0 &= (-a_0 \delta_0^2 + a_3 \delta_1^2 + a_4 \delta_1 \delta_2 + a_5 \delta_2^2) p_0 + \\ &\quad (-a_1 \delta_0^2 - 2a_3 \delta_0 \delta_1 - a_4 \delta_0 \delta_2) p_1 + \\ &\quad (-a_2 \delta_0^2 - a_4 \delta_0 \delta_1 - 2a_5 \delta_0 \delta_2) p_2 \\ r_1 &= (-2a_0 \delta_0 \delta_1 - a_1 \delta_1^2 - a_2 \delta_1 \delta_2) p_0 + \\ &\quad (a_0 \delta_0^2 + a_2 \delta_0 \delta_2 - a_3 \delta_1^2 + a_5 \delta_2^2) p_1 + \\ &\quad (-a_2 \delta_0 \delta_1 - a_4 \delta_1^2 - 2a_5 \delta_1 \delta_2) p_2 \\ r_2 &= (-2a_0 \delta_0 \delta_2 - a_1 \delta_1 \delta_2 - a_2 \delta_2^2) p_0 + \\ &\quad (-a_1 \delta_0 \delta_2 - 2a_3 \delta_1 \delta_2 - a_4 \delta_2^2) p_1 + \\ &\quad (a_0 \delta_0^2 + a_1 \delta_0 \delta_1 + a_3 \delta_1^2 - a_5 \delta_2^2) p_2 \end{aligned}$$

5. Wir machen den Ansatz $\delta_0 = 0$. Dann ist $\lambda = \frac{q_0}{p_0}$ und
$$\delta_1 = q_1 - (\frac{p_1}{p_0})q_0, \quad \delta_2 = q_2 - (\frac{p_2}{p_0})q_0.$$
Der Satz über diophantische Approximationen sagt, daß es $(q_0, q_1, q_2) \in \mathbf{Z}^3 \setminus \{0\}$ gibt mit
$$|q_0| < p_0, \quad |\delta_1| \leq \frac{1}{\sqrt{p_0}}, \quad |\delta_2| \leq \frac{1}{\sqrt{p_0}}.$$
Dann gilt für $i = 1, 2$:
$$|q_i| = |\frac{p_i}{p_0} q_0 + \delta_i| < |q_0| + 1,$$
also $|q_i| \leq |q_0| < p_0$ und damit $H(Q) < H(P)$. Insbesondere ist dann nach Wahl von P der Punkt $Q \notin C(\mathbf{Q})$.
6. Wir betrachten jetzt nochmals die r_i's mit $\delta_0 = 0$:
$$\begin{aligned} r_0 &= (a_3\delta_1^2 + a_4\delta_1\delta_2 + a_5\delta_2^2)p_0 \\ r_1 &= (-a_1\delta_1^2 - a_2\delta_1\delta_2)p_0 + (-a_3\delta_1^2 + a_5\delta_2^2)p_1 + (-a_4\delta_1^2 - 2a_5\delta_1\delta_2)p_2 \\ r_2 &= (-a_1\delta_1\delta_2 - a_2\delta_2^2)p_0 + (-2a_3\delta_1\delta_2 - a_4\delta_2^2)p_1 + (a_3\delta_1^2 - a_5\delta_2^2)p_2 \end{aligned}$$
Wir schätzen jetzt mit der Dreiecksungleichung unter Beachtung von
$$|a_i| \leq H(C), \quad |p_i| \leq H(P), \quad H(P) \leq H(R), \quad |\delta_i\delta_j| \leq (\frac{1}{\sqrt{p_0}})^2 = \frac{1}{H(P)}$$
ab:
$$H(P) \leq H(R) \leq \max(|r_0|, |r_1|, |r_2|) \leq 7H(C)H(P)\frac{1}{H(P)},$$
woraus sofort $H(P) \leq 7H(C)$ folgt. ■

Wie gut ist diese Abschätzung. Dazu geben wir folgendes Beispiel:

Beispiel: Sei $f = x_0^2 - (x_1 - ax_0)^2 - (x_2 - ax_1)^2$ mit $a \in \mathbf{Z}$ und $a \geq 2$ und $C = \{f = 0\}$. Es ist
$$f = (-a^2 + 1)x_0^2 + 2ax_0x_1 + (-1 - a^2)x_1^2 + 2ax_1x_2 - x_2^2,$$
also
$$H(C) = a^2 + 1.$$
Wir wollen Punkte in $C(\mathbf{Q})$ bestimmen:
- Sei $P = (p_0 : p_1 : p_2) \in C(\mathbf{Q})$ mit $p_i \in \mathbf{Z}$. Dann gilt
$$p_0^2 = u^2 + v^2 \text{ mit } p_1 - ap_0 = u \text{ und } p_2 - ap_1 = v,$$
also
$$p_1 = ap_0 + u, \quad p_2 = a^2p_0 + au + v$$
und
$$P = (p_0 : ap_0 + u : a^2p_0 + au + v).$$
- Wäre $p_0 = 0$, so auch $u = v = 0$, was nicht sein kann. Also o.E. $p_0 \geq 1$.
- Wir geben zunächst nur ein paar Beispiele, indem wir zu p_0 Lösungen für u und v bestimmen. O.E. $ggT(p_0, u) = 1$, sonst läßt sich kürzen. Die kleinsten Lösungen für p_0 sind
$$(p_0, \pm u, \pm v) = (1, 0, 1), (1, 1, 0), (5, 3, 4), (5, 4, 3), (13, 5, 12), (13, 12, 5),$$
was auf die Lösungen
$$\begin{aligned} &(1 : a : a^2 \pm 1), (1 : a \pm 1 : a^2 \pm a), \\ &(5 : 5a \pm 3 : 5a^2 \pm 3 \pm 4), (5 : 5a \pm 4 : 5a^2 \pm 4 \pm 3), \\ &(13 : 13a \pm 5 : 13a^2 \pm 5 \pm 12), (13 : 13a \pm 12 : 13a^2 \pm 12 \pm 5), \end{aligned}$$
führt.

- Untersucht man jetzt bei festem p_0 und a die reelle Funktion $p_2(u,v) = a^2p_0 + au + v$ unter der Nebenbedingung $p_0^2 = u^2 + v^2$, so findet man
$$(a^2 - \sqrt{a^2+1})p_0 \leq p_2 \leq (a^2 + \sqrt{a^2+1})p_0.$$
(Man setzt an $g = (a^2p_0 + au + v) - t(p_0^2 - u^2 - v^2)$. Dann ist $\frac{\partial g}{\partial u} = a + 2tu$ und $\frac{\partial g}{\partial v} = 1 + 2tv$. Diese Ableitungen müssen 0 sein, woraus man $t = -\frac{1}{2v}$ und $u = av$ berechnet. Einsetzen in $p_0^2 = u^2 + v^2$ liefert $v^2 = \frac{p_0^2}{a^2+1}$, was die zwei Punkte
$$(u,v) = \pm\left(\frac{ap_0}{\sqrt{a^2+1}}, \frac{p_0}{\sqrt{a^2+1}}\right)$$
liefert. In diesen zwei Punkten wird p_2 extremal, nimmt dort die Werte $(a^2 \pm \sqrt{a^2+1})p_0$ an, was die Behauptung liefert.)
- Man sieht jetzt leicht, daß $P_{min} = (1 : a-1 : a^2-a)$ die kleinste Lösung ist. Es ist $H(P_{min}) = a^2-a$, also
$$\frac{H(P_{min})}{H(C)} = \frac{a^2-a}{a^2+1},$$
was für $a \to \infty$ gegen 1 geht.

Dies bedeutet, daß bei unserer Abschätzung höchstens noch die Konstante 7 verbessert werden kann.

KAPITEL 8

Kurven vom Geschlecht 1 — elliptische Kurven

Sofern nichts anderes gesagt, verstehen wir unter einer Kurve immer eine über dem Grundkörper K definierte absolut irreduzible nichtsinguläre projektive Kurve.

Beispiel: Ist $C \subseteq \mathbf{P}^2$ eine nichtsinguläre Kubik,

$$C = \{a_0x_0^3 + a_1x_0^2x_1 + a_2x_0^2x_2 + \cdots + a_9x_2^3 = 0\},$$

so hat C Geschlecht $g = \frac{(3-1)(3-2)}{2} = 1$.

Was können wir allgemein über eine Kurve C vom Geschlecht $g = 1$ sagen?

1. Für kanonische Divisoren gilt: $deg(K_C) = 2g - 2 = 0$ und $\ell(K_C) = g = 1$. Sei $f \in \mathcal{L}(K_C) \setminus \{0\}$. Dann gilt $K_C + (f) \geq 0$. Wegen $deg(K_C + (f)) = deg(K_C) = 0$ gilt bereits $K_C + (f) = 0$, also ist auch der triviale Divisor 0 kanonisch. Wir können also stets $K_C = 0$ annehmen.
2. Der Satz von Riemann-Roch wird dann zu
$$\ell(D) = deg(D) + \ell(-D).$$
Insbesondere folgt
$$\ell(D) = deg(D) \quad \text{für } deg(D) \geq 1.$$
3. Wie kann man C als projektive Kurve realisieren? Im Fall $g(C) = 0$ war $C \simeq \phi_{-K}(C) \subseteq \mathbf{P}^2$ eine ebene Quadrik. Im Fall $g(C) = 1$ haben wir leider keinen natürlichen über K definierten Divisor zur Verfügung. (Ich weiß keine Antwort auf diese Frage.)

Es gibt Kurven vom Geschlecht 0 über $\mathbf{Q}$, die keine $\mathbf{Q}$-rationalen Punkt besitzen, wie folgendes Beispiel zeigt.

Beispiel: Sei $\alpha \in \mathbf{F}_8$ mit $\alpha^3 + \alpha + 1 = 0$. Es ist $\mathbf{F}_8 = \mathbf{F}_2(\alpha)$. Wir betrachten über $\mathbf{F}_2$ ($x \mapsto x^2$ ist der Frobeniusautomorphismus, $x \mapsto x^2$ und $x \mapsto x^4$ also die nichttrivialen Elemente der Galoisgruppe):

$$f = (x_0 + \alpha x_1 + \alpha^2 x_2)(x_0 + \alpha^2 x_1 + \alpha^4 x_2)(x_0 + \alpha^4 x_1 + \alpha^8 x_2).$$

Ausmultiplizieren liefert

$$f = x_0^3 + x_0x_1^2 + x_0x_1x_2 + x_0x_2^2 + x_1^3 + x_1x_2^2 + x_2^3.$$

$\{f = 0\} \subseteq \mathbf{P}^2$ hat also keinen $\mathbf{F}_2$-rationalen Punkt, zerfällt über $\mathbf{F}_8$ in 3 Geraden.
Wir definieren jetzt über $\mathbf{Q}$:

$$F = x_0^3 + x_0x_1^2 + x_0x_1x_2 + x_0x_2^2 + x_1^3 + x_1x_2^2 + x_2^3$$

und $C = \{F = 0\} \subseteq \mathbf{P}^2$. Man rechnet nach, daß C nichtsingulär ist. Da F modulo 2 keine nichttrivialen Nullstellen hat, hat C keine $\mathbf{Q}$-rationalen Punkte, wie man durch Reduktion modulo 2 sieht.

Wir betrachten jetzt Kurven vom Geschlecht 1 mit einem K-rationalen Punkt.

Definition 37. *Eine elliptische Kurve E über K ist eine Kurve vom Geschlecht 1 zusammen mit einem Punkt $O \in E(K)$.*

Da wir jetzt bei elliptischen Kurven nichttrivaiale über K definierte Divisoren kennen, können wir sie als projektive Kurven realisieren:

SATZ 43. *Sei (E, O) eine elliptische Kurve über K. Dann ist E über K isomorph zu einer ebenen Kubik der Gestalt*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

mit $a_i \in K$, wobei O dem Punkt $(0 : 0 : 1)$ entspricht. Eine solche Gleichung nennt man auch eine Weierstraßgleichung für E.

Beweis:

1. Wir wissen, daß ein ϕ_D mit $deg(D) \geq 2g + 1 = 3$ eine Einbettung als Kurve vom Grad $deg(D)$ in $\mathbf{P}^{\ell(D)-1}$ liefert. Wir wählen den über K definierten Divisor $D = 3 \cdot O$. Riemann-Roch liefert $\ell(3 \cdot O) = 3$, also erhalten wir
$$E \simeq \phi_{3O}(E) \subseteq \mathbf{P}^2$$
als Kurve vom Grad 3 im $\mathbf{P}^2$.
2. Wie sieht ϕ_{3O} aus? Riemann-Roch liefert $\ell(nO) = n$ für $n \geq 1$. Sei t uniformisierend in O und $v = v_O$ die zugehörige Bewertung. Wir beschreiben jetzt diese $\mathcal{L}(nO)$'s:
Natürlich ist $\mathcal{L}(O) = [1]$, wo die Klammern den über $\overline{K}$ aufgespannten Vektorraum bezeichnen.
Wegen $\ell(2O) = 2$ gibt es ein $x \in K(E)$ mit $\mathcal{L}(2O) = [1, x]$. Wegen $x \notin \mathcal{L}(O)$ ist $v(x) = -2$ und wir können nach Multiplikation mit einer Konstanten $(t^2x)(O) = 1$ erreichen.
Analog erhält man ein $y \in K(E)$ mit $\mathcal{L}(3O) = [1, x, y]$. Die Funktion y erfüllt $v(y) = -3$, also können wir wieder o.E. $(t^3y)(O) = 1$ annehmen. x und y haben außer in O keine Polstelle. Wir definieren jetzt $\phi = \phi_{3O} = (1 : x : y)$. Was ist $\phi(O)$? Es ist $\phi = (t^3 : t(t^2x) : t^3y)$, also wegen $t(O) = 0$:
$$\phi(O) = (0 : 0 : 1).$$
$\phi(E)$ ist eine zu E isomorphe ebene Kurve vom Grad 3. Wir brauchen jetzt nur noch eine nichttriviale Relation zwischen $1, x, y$ um die Kurvengleichung zu erhalten.
3. Es gilt weiter
$$\mathcal{L}(4O) = [1, x, y, x^2], \quad \mathcal{L}(5O) = [1, x, y, x^2, xy], \mathcal{L}(6O) = [1, x, y, x^2, xy, x^3].$$
Nun ist $y^2 \in \mathcal{L}(6O) \setminus \mathcal{L}(5O)$, also gibt es $a_1, a_2, a_3, a_4, a_6, c \in K$, $c \neq 0$ mit
$$y^2 = cx^3 + a_2x^2 + a_4x + a_6 - a_1xy - a_3y.$$
Multipliziert man mit t^6 und setzt dann O ein, so erhält man
$$(t^3y)^2(O) = c(t^2x)^3(O) + 0,$$
also $c = 1$. Damit haben wir
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$
Dieser Gleichung genügt dann auch $\phi(E)$ in $\mathbf{P}^2$, was wir noch zeigen wollten. ■

Aufgabe: Sei $C = \{f = 0\}$ über $\mathbf{Q}$ definiert durch

$$f = 3x_0^2x_1 + x_0x_1^2 + 3x_0x_1x_2 + x_0x_2^2 - x_1^3 + 2x_1^2x_2 - x_2^3.$$

C hat den $\mathbf{Q}$ rationalen Punkt $O = (1 : 0 : 0)$ und ist nichtsingulär. Bestimme den durch ϕ_{3O} definierten Morphismus sowie die Gleichung des Bildes.

FOLGERUNG 15. *Ist $char(K) \neq 2, 3$ und (E, O) eine elliptische Kurve über K, so ist E isomorph zu einer ebenen Kurve*

$$y^2 = x^3 + ax + b$$

mit $a, b \in K$, wo O dem Punkt $(0 : 0 : 1)$ entspricht.

Beweis: Wir können mit einer Gleichung

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

starten. Das Ziel erreichen wir durch quadratische und kubische Ergänzung. Wir können auch einen Koordinatenwechsel ansetzen:

$$y = y' + Ax' + B, \quad x = x' + C.$$

Wählt man

$$A = -\frac{1}{2}a_1, \quad B = -\frac{1}{2}a_3 + \frac{1}{6}a_1a_2 + \frac{1}{24}a_1^3, \quad C = -\frac{1}{3}a_2 - \frac{1}{12}a_1^2,$$

so erhält man eine Gleichung $y'^2 = x'^3 + ax' + b$ der gewünschten Form. ■

Während für Kurven vom Geschlecht 0 die Picardgruppe Pic^0 trivial ist, gilt für Kurven vom Geschlecht 1 folgender Satz:

SATZ 44. *Sei (E, O) eine elliptische Kurve. Dann ist die Abbildung*

$$\psi : E \to Pic^0(E), \quad P \mapsto \textit{Klasse von } P - O$$

eine Bijektion.

Beweis: ψ ist surjektiv: Sei D ein Divisor vom Grad 0. Dann hat $D + O$ Grad 1, nach Riemann-Roch ist $\ell(D + O) = 1$, also gibt es eine Funktion $f \in \overline{K}(E)$ mit $D + O + (f) \geq 0$. Der Divisor $D + O + (f)$ ist effektiv vom Grad 1, also ein Punkt: $D + O + (f) = P$. Damit gilt $D \sim P - O$, also Klasse von $D = \psi(P)$. *ψ ist injektiv:* Sei $\psi(P) = \psi(Q)$. D.h. $P - O \sim Q - O$, es gibt also eine Funktion f mit $P - O = Q - O + (f)$ und damit $(f) = P - Q$. Also ist $f \in \mathcal{L}(Q) = \overline{K}$ und damit $P = Q$. ■

Diese Bijektion erlaubt uns jetzt eine Gruppenstruktur auf (E, O) einzuführen:

DEFINITION 38. *Sei (E, O) eine elliptische Kurve und $\psi : E \to Pic^0(E), P \mapsto P - O$. Für P_1, P_2 definieren wir*

$$P_1 \oplus P_2 = \psi^{-1}(\psi(P_1) + \psi(P_2)).$$

Dadurch wird E zu einer abelschen Gruppe mit O als neutralem Element.

Bemerkungen:

- Wir werden später einfach $P_1 + P_2$ statt $P_1 \oplus P_2$ schreiben, wenn klar ist, daß nicht der Divisor $P_1 + P_2$ vom Grad 2 gemeint ist.
- Für $P, Q, R \in E$ gilt:

$$\begin{aligned} P \oplus Q = R \quad &\Longleftrightarrow \quad \psi(P) + \psi(Q) = \psi(R) \\ &\Longleftrightarrow \quad P - O + Q - O \sim R - 0 \\ &\Longleftrightarrow \quad P + Q \sim O + R \Longleftrightarrow R \sim P + Q - O. \end{aligned}$$

  Wie findet man also R? Der Divisor $P + Q - O$ hat Grad 1, also ist $\mathcal{L}(P + Q - O)$ 1-dimensional. Sei $\mathcal{L}(P + Q - O) = \overline{K}f$. Dann ist $P + Q - O + (f)$ effektiv vom Grad 1, also ein Punkt, nämlich R.
- Aus der Überlegung eben folgt sofort, daß $E(K)$ abgeschlossen bzgl. $\oplus$ ist, also eine Untergruppe.
- Das inverse Element zu P ist durch die Gleichung $P + P' \sim 2O$ bestimmt.

Wir wollen für ebene Kubiken die Gruppenstruktur geometrisch deuten, wozu wir ein paar Aussagen über Geradenschnitte brauchen:

LEMMA 10. *Sei $E \subseteq \mathbf{P}^2$ eine nichtsinguläre Kurve vom Grad 3 und $H = (h)$ ein Geradenschnitt, insbesondere $deg(H) = 3$. Dann gilt: Ist D ein effektiver Divisor, der linear äquivalent zu H ist, so ist D selbst schon ein Geradenschnitt, d.h. es gibt eine Gerade $g = b_0x_0 + b_1x_1 + b_2x_2 = 0$ mit $D = (g)$.*

Beweis: Nach Riemann-Roch gilt $\ell(H) = deg(H) = 3$, also ist

$$\mathcal{L}(H) = [\frac{x_0}{h}, \frac{x_1}{h}, \frac{x_2}{h}].$$

Wegen $D \sim H$ gibt es eine Funktion f mit $D = H + (f)$. Wegen $D \geq 0$ ist $f \in \mathcal{L}(H)$, also gibt es $b_0, b_1, b_2 \in \overline{K}$ mit

$$f = \frac{b_0x_0 + b_1x_1 + b_2x_2}{h},$$

woraus sofort $D = (b_0x_0 + b_1x_1 + b_2x_2)$ folgt. ■

Aufgabe: Zeige die analoge Aussage für alle nichtsingulären ebenen Kurven. Die entsprechende Eigenschaft wird auch lineare Normalität genannt.

Geometrische Deutung der Addition für nichtsinguläre ebene Kubiken: Sei $E = \{f = 0\} \subseteq \mathbf{P}^2$ eine nichtsinguläre Kurve vom Grad 3 und $O \in E(K)$. Wie kann man die oben definierte Addition beschreiben?

1. Seien P und Q Punkte auf E. Dann gibt es eine eindeutig bestimmte Gerade $g = 0$ und einen weiteren Punkt $R' \in E$ mit
$$P + Q + R' = (g).$$
$g = 0$ ist die Gerade durch P und Q bzw. die Tangente in P an E im Fall $P = Q$.
2. Analog gibt es eine eindeutig bestimmte Gerade $h = 0$ durch O und R' und einen weiteren Punkt $R \in E$ mit
$$O + R' + R = (h).$$
Im Fall $O = R'$ ist $h = 0$ die Tangente in O an E.
3. Nun wollen wir $P \oplus Q$ bestimmen. Es gilt für $S \in E$:
$$\begin{aligned} P \oplus Q = S \quad &\iff \quad P - O + Q - O \sim S - O \iff S + O \sim P + Q \\ &\iff \quad S + O + R' \sim P + Q + R' \sim (g) \\ &\iff \quad S + O + R' \text{ ist Geradenschnitt nach dem Lemma} \\ &\iff \quad S + O + R' = (h) = R + O + R' \\ &\iff \quad S = R. \end{aligned}$$
Damit gilt also $R = P \oplus Q$.
4. Wir wollen noch das Inverse zu $P \in E$ bestimmen. Sei dazu $g = 0$ die Tangente in O an E und $(g) = 2O + O'$.
$$\begin{aligned} P \oplus P' = O \quad &\iff \quad P - O + P' - O \sim O - O \\ &\iff \quad P + P' \sim 2O \\ &\iff \quad P + P' + O' \sim 2O + O' = (g) \\ &\iff \quad P + O' + P' \text{ ist Geradenschnitt} \end{aligned}$$
Ist $h = 0$ die Gerade durch P und O', so ist also P' eindeutig bestimmt durch $P + O' + P' = (h)$.

Wir fassen zusammen:

SATZ 45. *Sei E eine nichtsinguläre ebene Kubik und $O \in E(K)$.*

1. *Die Addition zweier Punkte $P, Q \in E$ ergibt sich geometrisch wie folgt:*
   - *Bestimme die Gerade $g = 0$ durch P und Q und damit den 3. Schnittpunkt R' mit $(g) = P + Q + R'$.*
   - *Bestimme die Gerade $h = 0$ durch R' und O und damit den 3. Schnittpunkt R mit $(h) = R' + O + R$.*

   Dann gilt $P \oplus Q = R$.
2. *Bestimme die Tangente $t = 0$ in O an E und damit den 3. Schnittpunkt O' mit $(t) = 2O + O'$. Bestimme für $P \in E$ die Gerade $s = 0$ durch P und O' und damit den 3. Schnittpunkt P' mit $(s) = P + O' + P'$. Dann ist $\ominus P = P'$.*

Beispiel: Wir betrachten wieder $E = \{f = 0\}$ über $\mathbf{Q}$ mit
$$f = 3x_0^2x_1 + x_0x_1^2 + 3x_0x_1x_2 + x_0x_2^2 - x_1^3 + 2x_1^2x_2 - x_2^3$$
und $O = (1 : 0 : 0)$.

1. Die Tangente in O ist $x_1 = 0$, woraus man schnell $O' = (1 : 0 : 1)$ errechnet.
2. Wir wollen $2 \cdot O' = O' \oplus O'$ berechnen. Die Tangente in O' ist $x_0 + 6x_1 - x_2 = 0$, einsetzen in f liefert
$$f(x_0, x_1, x_0 + 6x_1) = -x_1^2(205x_1 + 51x_0),$$
woraus sich als 3. Schnittpunkt mit der Tangente $R' = (205 : -51 : -101)$ ergibt. Die Gerade zwischen O und R' hat die Gleichung $x_2 = \frac{101}{51}x_1$, mit
$$f(x_0, x_1, \frac{101}{51}x_1) = \frac{1}{132651}x_1(5x_0 + 205x_1)(7803x_0 - 3110x_1)$$

erhält man als 3. Schnittpunkt $R = (3110 : 7803 : 15453)$, also

$$2 \cdot (1 : 0 : 1) = (3110 : 7803 : 15453).$$

(Über $\mathbf{R}$ ist $(205 : -51 : -101) \approx (1 : -0.25 : -0.49)$ und $(3110 : 7803 : 15453) \approx (1 : 2.51 : 4.97)$.)

3. Wir berechnen jetzt $(1 : 0 : 1) \oplus (3110 : 7803 : 15453)$: Die Gerade durch die beiden Punkte ist

$$x_2 = x_0 + \frac{12343}{7803} x_1,$$

einsetzen in f liefert

$$\frac{1}{475099770627} x_1 (269008425 x_0 + 274115666 x1)(7803 x_0 - 3110 x_1),$$

so daß man für den 3. Schnittpunkt

$$(274115666 : -269887425 : -151409259)$$

erhält. Die Gerade durch diesen Punkt und O ist

$$x_2 = \frac{989603}{1758225} x_1,$$

sie schneidet E in dem 3. Punkt

$$3 \cdot (1 : 0 : 1) = (1043360347 : 60614806875 : 34116563425).$$

4. So kann man weitermachen. Allerdings werden die Höhen der auftretenden Punkte schnell sehr groß. Die folgenden Zahlen geben $\frac{1}{m^2} \ln H(m \cdot (1 : 0 : 1))$ an für $m = 1, \ldots$:

$$0, \quad 2.41, \quad 2.76, \quad 3.05, \quad 3.15, \quad 3.27, \quad 3.32, \quad 3.38, \quad 3.41, \quad 3.44, \ldots$$

Steckt dahinter eine Gesetzmäßigkeit?
5. Die Addition kann man natürlich auch einfach programmieren, was wir auch für die folgenden Rechnungen gemacht haben.
6. Welche $\mathbf{Q}$-rationalen Punkte hat E? Mit UBASIC haben wir bis Höhe 340 gesucht und die Punkte gefunden, die in beigefügter Tabelle stehen. Dabei steht Pn für einen Punkt der Höhe n. Gibt es mehrere, haben wir sie mit $a, b, c, \ldots$ durchnumeriert.
7. Da $E(\mathbf{Q})$ eine Gruppe bildet, kann man natürlich fragen, welche Struktur diese Gruppe hat. Wir haben $O = (1 : 0 : 0) = P1a$ und $O' = (1 : 0 : 1) = P1b$. Nach einem mißlungenen Versuch haben wir

$$A_1 = (1 : 0 : 1) = P1b, \quad A_2 = (1 : 1 : -1) = P1d, \quad A_3 = (3 : -4 : 2) = P4$$

gewählt, womit sich alle gefundenen Punkte der Tabelle linear kombinieren ließen. (In der Tabelle stehen bei jedem Punkt die Koeffizienten n_1, n_2, n_3 von $P = n_1 A_1 + n_2 A_2 + n_3 A_3$.) Die Frage stellt sich jetzt: Gilt

$$E(\mathbf{Q}) = \mathbf{Z} A_1 + \mathbf{Z} A_2 + \mathbf{Z} A_3,$$

bzw. $E(\mathbf{Q}) \simeq \mathbf{Z}^3$?

Geometrische Addition für $y^2 = x^3 + ax + b$:

- E sei also affin gegeben durch $f = 0$ mit $f = x^3 + ax + b - y^2$ bzw. projektiv durch $F = 0$ mit $F = x_1^3 + a x_0^2 x_1 + b x_0^3 - x_0 x_2^2$ und $O = (0 : 0 : 1)$. Wir setzen weiter voraus, daß die Charakteristik $\neq 2, 3$ ist.
- Wann ist E singulär? Es gilt

$$\frac{\partial F}{\partial x_0} = 2a x_0 x_1 + 3b x_0^2 - x_2^2, \quad \frac{\partial F}{\partial x_1} = 3x_1^2 + a x_0^2, \quad \frac{\partial F}{\partial x_2} = -2 x_0 x_2.$$

Wäre $x_0 = 0$, so würde $x_1 = x_2 = 0$ folgen, was nicht geht. Also o.E. $x_0 = 1$ und $x_1 = x$, $x_2 = y$. Es folgt $y = 0$ und $2ax + 3b = 0$, $3x^2 + a = 0$. Für $a = 0$ erhält man $b = 0$ und $x = 0$, für $a \neq 0$ durch Elimination $x = -\frac{3b}{2a}$ und die Bedingung $4a^3 + 27b^2 = 0$. Definiert man

$$\Delta = 4a^3 + 27b^2,$$

so kann man dies zusammenfassen:

$$E \text{ ist singulär} \iff \Delta = 0.$$

P	Punkt	$P = n_1A_1 + n_2A_2 + n_3A_3$
$P1a$	$(1:0:0)$	$0,0,0$
$P1b$	$(1:0:1)$	$1,0,0$
$P1c$	$(0:1:1)$	$0,2,-1$
$P1d$	$(1:1:-1)$	$0,1,0$
$P3a$	$(1:1:3)$	$1,-2,0$
$P3b$	$(2:-3:3)$	$1,-1,0$
$P4$	$(3:-4:2)$	$0,0,1$
$P5a$	$(4:-5:-1)$	$0,-2,1$
$P5b$	$(5:-3:-3)$	$1,-2,1$
$P5c$	$(5:-4:-3)$	$-1,2,0$
$P6$	$(5:6:-3)$	$1,0,-1$
$P9$	$(1:6:9)$	$0,-1,1$
$P11$	$(11:-4:-6)$	$1,1,-1$
$P12$	$(7:12:-2)$	$1,-3,1$
$P13$	$(3:8:-13)$	$0,-1,0$
$P21$	$(19:-21:-9)$	$0,1,-1$
$P22$	$(22:-3:-9)$	$0,2,0$
$P46$	$(19:-36:46)$	$-1,3,-1$
$P48$	$(1:-48:-36)$	$2,-2,0$
$P49$	$(4:49:21)$	$1,-1,1$
$P51$	$(7:-33:51)$	$-1,0,1$
$P54$	$(41:-54:9)$	$0,3,-1$
$P57$	$(22:57:3)$	$-1,1,0$
$P75$	$(19:75:15)$	$1,2,-1$
$P92$	$(11:92:34)$	$0,0,-1$
$P101$	$(101:-3:69)$	$-1,4,-1$
$P120$	$(120:-1:23)$	$2,-4,1$
$P135$	$(47:-100:135)$	$1,-4,2$
$P147$	$(109:-147:91)$	$1,2,-2$
$P152$	$(152:-3:53)$	$-1,1,1$
$P159$	$(79:30:159)$	$-1,2,-1$
$P187$	$(76:121:-187)$	$2,0,-1$
$P189$	$(170:189:-117)$	$0,-2,2$
$P205$	$(205:-51:-101)$	$-1,0,0$
$P209$	$(209:-196:-119)$	$2,-3,0$
$P236$	$(236:-9:-61)$	$1,-1,-1$
$P311$	$(311:-4:79)$	$0,3,-2$
$P312$	$(-7:-192:312)$	$1,1,0$
$P319$	$(319:-42:-129)$	$1,-4,1$
$P324$	$(-211:-240:324)$	$0,4,-2$
$P336$	$(1:336:204)$	$-1,3,0$

$\mathbf{Q}$-rationale Punkte der Höhe ≤ 340 auf
$E = \{3x_0^2x_1 + x_0x_1^2 + 3x_0x_1x_2 + x_0x_2^2 - x_1^3 + 2x_1^2x_2 - x_2^3 = 0\}$.

- Der einzige unendlich ferne Punkt, d.h. Punkt auf der Geraden $x_0 = 0$ ist O. Damit folgt auch sofort $O' = O$. Die Geraden durch O haben die Form $c_0x_0 + c_1x_1 = 0$, außer x_0 sind dies also die Geraden $x = c$ mit $c \in \overline{K}$.
- Was ist $\ominus P$ für $P = (x_0, y_0)$? Die Gerade durch P und O' hat die affine Gleichung $x = x_0$, einsetzen in f liefert

$$f(x_0, y) = x_0^3 + ax_0 + b - y^2 = y_0^2 - y^2 = -(y - y_0)(y + y_0).$$

Also ist der 3. Punkt auf der Geraden $(x_0, -y_0)$ und es folgt

$$\ominus(x_0, y_0) = (x_0, -y_0).$$

- Seien $P_1 = (x_1, y_1)$ und $P_2 = (x, y_2)$ Punkte auf E. Wir wollen $P_1 \oplus P_2$ berechnen. Gilt $x_1 = x_2$ und $y_2 = -y_1$, so ist $P_1 \oplus P_2 = O$, also können wir voraussetzen, daß dieser Fall nicht vorliegt. Im Fall $x_1 = x_2$ ist also $y_1 = y_2 \neq 0$.
- Sei $y = \lambda x + \mu$ die Gerade und P_1 und P_2. Zunächst ist immer $\mu = y_1 - \lambda x_1$. Ist $P_1 \neq P_2$, so ist
$$\lambda = \frac{y_1 - y_2}{x_1 - x_2}.$$
Ist $P_1 = P_2$, so müssen wir die Tangente berechnen, also
$$\frac{\partial f}{\partial x}(P_1)(x - x_1) + \frac{\partial f}{\partial y}(P_1)(y - y_1) = 0,$$
bzw.
$$y - y_1 = \frac{3x_1^2 + a}{2y_1}(x - x_1),$$
woraus sofort
$$\lambda = \frac{3x_1^2 + a}{2y_1}$$
folgt.
- Wir berechen den 3. Schnittpunkt $(\tilde{x}, \tilde{y})$ mit der Geraden und setzen dazu $y = \lambda x + \mu$ in f ein:
$$f(x, \lambda x + \mu) = x^3 + ax + b - (\lambda x + \mu)^2 = x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + (b - \mu^2).$$
Dies muß gleich dem Polynom
$$(x - x_1)(x - x_2)(x - \tilde{x}) = x^3 - (x_1 + x_2 + \tilde{x})x^2 + \dots$$
sein, woraus durch Koeffizientenvergleich bei x^2 sofort
$$\tilde{x} = \lambda^2 - x_1 - x_2 \text{ und damit } \tilde{y} = \lambda\tilde{x} + \mu$$
folgt. Der 3. Schnittpunkt auf der Verbindungsgeraden von $(\tilde{x}, \tilde{y})$ und O ist $(\tilde{x}, -\tilde{y})$, also folgt schließlich für $(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$:
$$x_3 = \lambda^2 - x_1 - x_2 \text{ und } y_3 = -\lambda x_3 - \mu.$$
- Damit sieht man jetzt auch: $P_1 \oplus P_2 \oplus P_3 = O$ genau dann, wenn P_1, P_2, P_3 auf einer Geraden liegen.

Wir fassen das Ergebnis zusammen:

Satz 46. *In Charakteristik $\neq 2, 3$ ist die Kurve $y^2 = x^3 + ax + b$ genau dann nichtsingulär, wenn $\Delta = 4a^3 + 27b^2 \neq 0$ gilt. In diesem Fall ist E mit dem Punkt $O = (0 : 0 : 1)$ eine elliptische Kurve, für die das Additionsgesetz wie folgt aussieht, wenn (x_i, y_i) Punkte auf E sind.*

$$\begin{aligned} \ominus(x_1, y_1) &= (x_1, -y_1) \\ (x_1, y_1) \oplus (x_1, -y_1) &= O \\ (x_1, y_1) \oplus (x_2, y_2) &= (x_3, y_3) \text{ mit} \\ & \quad x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = -\lambda x_3 - y_1 + \lambda x_1 \text{ und} \\ & \quad \lambda = \left\{ \begin{array}{cc} \frac{y_1 - y_2}{x_1 - x_2} & \text{für } x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1} & \text{für } x_1 = x_2 \text{ und } y_1 = y_2 \neq 0. \end{array} \right\} \end{aligned}$$

Außerdem gilt: $P_1 \oplus P_2 \oplus P_3 = O$ genau dann, wenn $P_1 + P_2 + P_3$ ein Geradenschnitt ist.

Beispiel: Sei E gegeben durch $y^2 = x^3 + 17$. Man findet $P = (-2, 3) \in E$ und rechnet mit den Formeln dann nach

$$P \oplus P = (8, -23), \quad P \oplus P \oplus P = (\frac{19}{25}, \frac{522}{125}).$$

Man suche mit dem Computer weitere Punkte und versuche die Gruppenstruktur von $E(\mathbf{Q})$ zu erraten.

Allgemeine Additionstheoreme: Ist E eine elliptische Kurve in Charakteristik $\neq 2, 3$, gegeben durch eine Gleichung $y^2 = x^3 + ax + b$ (mit $\Delta = 4a^3 + 27b^2 \neq 0$), so geben folgende Formeln die Addition an:

$$(z_{i0} : z_{i1} : z_{i2}) = (x_0 : x_1 : x_2) \oplus (y_0 : y_1 : y_2).$$

(Für jeden Punkt $P \in E$ gibt es mindestens ein i mit $(z_{i0}(P), z_{i1}(P), z_{i2}(P)) \neq 0$.)

```
z10 := a*x0^2*y0*y1-a*x0*x1*y0^2-x0^2*y2^2+x2^2*y0^2+3*x0*x1*y1^2
       -3*x1^2*y0*y1;
z11 := -3*b*x0^2*y0*y1+3*b*x0*x1*y0^2-a*x0^2*y1^2+a*x1^2*y0^2
       -x0*x1*y2^2+x2^2*y0*y1+2*x0*x2*y1*y2-2*x1*x2*y0*y2;
z12 := 3*b*x0^2*y0*y2-3*b*x0*x2*y0^2+a*x0^2*y1*y2-a*x1*x2*y0^2
       +2*a*x0*x1*y0*y2-2*a*x0*x2*y0*y1-x0*x2*y2^2+x2^2*y0*y2
       +3*x1^2*y1*y2-3*x1*x2*y1^2;

z20 := 3*b*x0^2*y0*y1-3*b*x0*x1*y0^2+a*x0^2*y1^2-a*x1^2*y0^2
       +x0*x1*y2^2-x2^2*y0*y1+2*x0*x2*y1*y2-2*x1*x2*y0*y2;
z21 := a^2*x0^2*y0*y1-a^2*x0*x1*y0^2-3*b*x0^2*y1^2+3*b*x1^2*y0^2
       -a*x0*x1*y1^2+a*x1^2*y0*y1+x1^2*y2^2-x2^2*y1^2;
z22 := -a^2*x0^2*y0*y2+a^2*x0*x2*y0^2+3*b*x0^2*y1*y2-3*b*x1*x2*y0^2
       +6*b*x0*x1*y0*y2-6*b*x0*x2*y0*y1+2*a*x0*x1*y1*y2
       -2*a*x1*x2*y0*y1-a*x0*x2*y1^2+a*x1^2*y0*y2+x1*x2*y2^2-x2^2*y1*y2;

z30 := 6*b*x0*x2*y0^2+6*b*x0^2*y0*y2+2*a*x1*x2*y0^2+2*a*x0^2*y1*y2
       +4*a*x0*x2*y0*y1+4*a*x0*x1*y0*y2+2*x2^2*y0*y2+2*x0*x2*y2^2
       +6*x1*x2*y1^2+6*x1^2*y1*y2;
z31 := 2*a^2*x0*x2*y0^2+2*a^2*x0^2*y0*y2-6*b*x1*x2*y0^2-6*b*x0^2*y1*y2
       -12*b*x0*x2*y0*y1-12*b*x0*x1*y0*y2-4*a*x1*x2*y0*y1
       -4*a*x0*x1*y1*y2-2*a*x1^2*y0*y2-2*a*x0*x2*y1^2+2*x2^2*y1*y2
       +2*x1*x2*y2^2;
z32 := -2*x0^2*y0^2*a^3-18*x0^2*y0^2*b^2-6*a*b*x0*x1*y0^2
       -6*a*b*x0^2*y0*y1-2*a^2*x1^2*y0^2-2*a^2*x0^2*y1^2
       -8*a^2*x0*x1*y0*y1+18*b*x1^2*y0*y1+18*b*x0*x1*y1^2+6*a*x1^2*y1^2
       +2*x2^2*y2^2;
```

Außerdem gilt:

$$\ominus(x_0 : x_1 : x_2) = (x_0 : x_1 : -x_2).$$

Damit erhält man:

FOLGERUNG 16. *Auf einer elliptischen Kurve E sind die Addition $E \times E \to E$ und die Inversenbildung $E \to E$ Morphismen.*

Indem man einen Punkt fest einsetzt, folgt:

FOLGERUNG 17. *Ist (E, O) eine elliptische Kurve und $P_0 \in E$, so ist die Translation*

$$\tau_{P_0} : E \to E, \quad P \mapsto P \oplus P_0$$

ein Isomorphismus. Es ist $\tau_{P_0}^{-1} = \tau_{\ominus P_0}$.

Wir wollen uns jetzt der Frage zuwenden, wieweit die Weierstraßgleichung einer elliptischen Kurve eindeutig bestimmt ist.

1. Seien (E, O) und (E', O') zwei elliptische Kurven in Weierstraßgleichung: $y^2 = x^3 + ax + b$ und ${y'}^2 = {x'}^3 + a'x' + b'$ und $\phi : E \to E'$ ein Isomorphismus. Indem wir ϕ eventuell um eine Translation abändern, können wir $\phi(O) = O'$ annehmen.
2. Es ist
$$\mathcal{L}(2O) = [1, x] \text{ und } \mathcal{L}(3O') = [1, x']$$
und
$$\mathcal{L}(3O) = [1, x, y] \text{ und } \mathcal{L}(3O') = [1, x', y'].$$

Da ϕ ein Isomorphismus ist, hat $\phi^*(O')$ Grad 1, also $\phi^*(O') = O$. Daher gilt für $n \in \mathbf{N}$ und $f \in \overline{K}(E')$:

$$f \in \mathcal{L}(nO') \Rightarrow (f) + nO' \geq 0 \Rightarrow 0 \leq (\phi^* f) + nO \Rightarrow \phi^* f \in \mathcal{L}(nO).$$

Wendet man dies für $n = 2, 3$ an, so sieht man, daß es $v, v_1, w, w_1, w_2 \in K$ gibt mit $v, w \neq 0$ und

$$\phi^* x' = x'' = vx + v_1 \text{ und } \phi^* y' = y'' = wy + w_1 x + w_2.$$

Natürlich gilt $y''^2 = x''^3 + a'x'' + b''$. Andererseits ist $y^2 = x^3 + ax + b$ die kleinste Relation zwischen x und y. Durch Einsetzen sieht man sofort, daß keine Terme xy und y auftreten, was $w_1 = w_2 = 0$ ergibt. Da auch kein Term x^2 auftritt, folgt auch $v_1 = 0$. Also bleibt $x'' = vx$ und $y'' = wy$. Wir setzten jetzt ein:

$$\begin{aligned} 0 &= x''^3 + a'x'' + b' - y''^2 = v^3 x^3 + a'vx + b' - w^2 y^2 = \\ &= v^3 x^3 + a'vx + b' - w^2(x^3 + ax + b) = \\ &= (v^3 - w^2)x^3 + (a'v - w^2 a)x + (b' - w^2 b), \end{aligned}$$

was durch Koeffizientenvergleich sofort

$$v^3 = w^2, \quad a'v = w^2 a, \quad b' = w^2 b$$

ergibt. Setzt man $u = \frac{w}{v}$, so ergibt sich

$$u^2 = v, \quad u^3 = w \text{ und } a' = u^4 a, \quad b' = u^6 b.$$

3. Gilt umgekehrt für ein $u \in K$, $u \neq 0$:

$$a' = u^4 a, \quad b' = u^6 b,$$

so führt der Koordinatenwechsel $(x, y) \mapsto (u^2 x, u^3 y)$ die Kurve E in E' über.

Damit haben wir bewiesen:

SATZ 47. *Zwei elliptische Kurven $E : y^2 = x^3 + ax + b$ und $E' : y^2 = x^3 + a'x + b'$ sind genau dann (über K) isomorph, wenn es ein $u \in K^\times$ gibt mit*

$$a' = u^4 a \text{ und } b' = u^6 b.$$

In diesem Fall liefert $(x, y) \mapsto (u^2 x, u^3 y)$ einen Isomorphismus $E \to E'$.

Wir werden nun eine wichtige Invariante einführen: Ist E eine elliptische Kurve und sind $y^2 = x^3 + ax + b$ und $y^2 = x^3 + a'x + b'$ zwei Weierstraßgleichungen für E, so gibt es also ein $u \in K$ mit $a' = u^4 a$ und $b' = u^6 b$. Für die Diskriminanten gilt:

$$\Delta' = 4a'^3 + 27b'^2 = u^{12} \Delta \neq 0$$

und damit

$$\frac{4a'^3}{4a'^3 + 27b'^2} = \frac{4a^3}{4a^3 + 27b^2}.$$

Daher ist dieser Ausdruck unabhängig von der Auswahl der Weierstraßgleichung und man definiert:

DEFINITION 39. *Ist E eine elliptische Kurve in Charakteristik $\neq 2, 3$ und $y^2 = x^3 + ax + b$ eine beschreibende Weierstraßgleichung, so definiert man die j-Invariante von E durch*

$$j = j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Aus obiger Überlegung folgt auch sofort:

FOLGERUNG 18. *Sind E und E' zwei über $\overline{K}$ isomorphe elliptische Kurven, so gilt: $j(E) = j(E')$.*

Elliptische Kurven zu vorgebener j-Invariante: Sei also $j \in K$ gegeben. Wir wollen sehen, ob es dazu elliptische Kurven gibt, und wie diese aussehen.

1. Wir gehen aus von $j = 1728 \frac{4a^3}{4a^3 + 27b^2}$. Zunächst ist klar:

$$j = 0 \quad \Longleftrightarrow \quad a = 0 \quad \text{und} \quad j = 1728 \quad \Longleftrightarrow \quad b = 0.$$

2. Wir setzen also jetzt $j \neq 0, 1728$ voraus. Dann haben wir die Umformungen:

$$\begin{aligned} j = 1728\frac{4a^3}{4a^3+27b^2} &\iff 4ja^3 + 27jb^2 = 1728 \cdot 4a^3 \\ &\iff 27jb^2 = 4(1728-j)a^3 \\ &\iff (\frac{b}{2})^2 = \frac{1728-j}{j}(\frac{a}{3})^3 \text{ und nach Multiplikation mit } (\frac{1728-j}{j})^2 \\ &\iff (\frac{1728-j}{2j}b)^2 = (\frac{1728-j}{3j}a)^3. \end{aligned}$$

Also gibt es wie üblich ein $t \in K$ mit

$$\frac{1728-j}{2j}b = t^3, \quad \frac{1728-j}{3j}a = t^2$$

oder anders geschrieben

$$a = \frac{3j}{1728-j}t^2, \quad b = \frac{2j}{1728-j}t^3.$$

3. Wann liefern t_1 und t_2 eine isomorphe Kurve? Genau dann, wenn es ein $u \in K^\times$ gibt mit

$$u^4 = \frac{a_{t_1}}{a_{t_2}} = (\frac{t_1}{t_2})^2 \quad \text{und} \quad u^6 = \frac{b_{t_1}}{b_{t_2}} = (\frac{t_1}{t_2})^3,$$

was nach Divison mit

$$u^2 = \frac{t_1}{t_2}$$

äquivalent ist.

Damit erhalten wir folgenden Satz:

Satz 48. 1. *Ist $j \in K$ und $j \neq 0, 1728$, so haben genau die Kurven E_t mit $y^2 = x^3 + a_t x + b_t$ und*

$$a_t = \frac{3j}{1728-j}t^2, \quad b_t = \frac{2j}{1728-j}t^3, \quad t \in K^\times$$

j-Invariante j. Weiterhin sind E_{t_1} und E_{t_2} genau dann isomorph über K, wenn es ein $u \in K$ gibt mit $t_2 = u^2 t_1$. Ist $t_\alpha, \alpha \in A$ ein Repräsentantensystem der Gruppe $K^\times/K^{\times 2}$, so repräsentieren die Kurven E_{t_α} alle Isomorphieklassen elliptischer Kurven über K mit j-Invariante j.

2. *Ist $j = 0$, so haben genau die Kurven E_b mit $y^2 = x^3 + b$ j-Invariante 0. Zwei Kurven E_{b_1} und E_{b_2} sind genau dann isomorph über K, wenn es ein $u \in K, u \neq 0$ gibt mit $b_2 = u^6 b_1$. Repräsentieren $b_\beta, \beta \in B$ die Klassen $K^\times/K^{\times 6}$, so die Kurven E_β die Isomorphieklassen elliptischer Kurven über K mit j-Invariante 0.*
3. *Ist $j = 1728$, so haben genau die Kurven E_a mit $y^2 = x^3 + ax$ j-Invariante 1728. Zwei Kurven E_{a_1} und E_{a_2} sind genau dann isomorph über K, wenn es ein $u \in K, u \neq 0$ gibt mit $a_2 = u^6 a_1$. Repräsentieren $a_\alpha, \alpha \in A$ die Klassen $K^\times/K^{\times 4}$, so die Kurven E_α die Isomorphieklassen elliptischer Kurven über K mit j-Invariante 1728.*

Folgerung 19. *Für elliptische Kurven E und E' gilt:*

$$E \sim_{\overline{K}} E' \quad \iff \quad j(E) = j(E').$$

Beispiel: Für $K = \mathbf{R}$ gilt

$$\mathbf{R}^{\times 2} = \mathbf{R}^{\times 4} = \mathbf{R}^{\times 6} = \{r \in R : r > 0\},$$

modulo zweiten, vierten und sechsten Potenzen bilden ± 1 ein Repräsentantensystem. Also erhält man folgendes Repräsentantensystem für die elliptischen Kurven über $\mathbf{R}$, wo j alle reellen Zahlen durchläuft:

$$\begin{aligned} j \neq 0, 1728: &\quad y^2 = x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j} \text{ und } y^2 = x^3 + \frac{3j}{1728-j}x - \frac{2j}{1728-j} \\ j = 0: &\quad y^2 = x^3 + 1 \text{ und } y^2 = x^3 - 1 \\ j = 1728: &\quad y^2 = x^3 + x \text{ und } y^2 = x^3 - x \end{aligned}$$

Beispiel: Für $K = \mathbf{F}_5$ gilt

$$\mathbf{F}_5^{\times 2} = \{1, 4\}, \quad \mathbf{F}_5^{\times 4} = \{1\}, \quad \mathbf{F}_5^{\times 6} = \{1, 4\},$$

also

$$\mathbf{F}_5^\times/\mathbf{F}_5^{\times 2} = \{\overline{1}, \overline{2}\}, \quad \mathbf{F}_5^\times/\mathbf{F}_5^{\times 4} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}, \quad \mathbf{F}_5^\times/\mathbf{F}_5^{\times 6} = \{\overline{1}, \overline{2}\}.$$

Damit erhält man folgende Tabelle:

j	Kurven E mit Anzahl von Punkten $\#E(\mathbf{F}_5)$
0	$y^2 = x^3 + 1 (N = 6), \quad y^2 = x^3 + 2 (N = 6)$
1	$y^2 = x^3 + 4x + 1 (N = 8), \quad y^2 = x^3 + x + 3 (N = 4)$
2	$y^2 = x^3 + x + 4 (N = 9), \quad y^2 = x^3 + 4x + 2 (N = 3)$
$1728 = 3$	$y^2 = x^3 \pm x (N = 4, 8), \quad y^2 = x^3 \pm 2x (N = 2, 10)$
4	$y^2 = x^3 + 3x + 2 (N = 5), \quad y^2 = x^3 + 2x + 1 (N = 7)$

(Beachte die symmetrische Verteilung der Anzahlen um 6.)

Aufgabe: Gib für $\mathbf{F}_{53}$ ein Repräsentantensystem der Isomorphieklassen elliptischer Kurven an und bestimme jeweils $\#E(\mathbf{F}_{53})$.

Beispiel: $K = \mathbf{F}_p$ ein endlicher Körper mit $p \geq 5$. Bezeichnet A die Anzahl der Isomorphieklassen elliptischer Kurven über $\mathbf{F}_p$, so gilt offensichtlich

$$A = (p-2)\#\mathbf{F}_p^\times/\mathbf{F}_p^{\times 2} + \#\mathbf{F}_p^\times/\mathbf{F}_p^{\times 4} + \#\mathbf{F}_p^\times/\mathbf{F}_p^{\times 6}.$$

Der Kern der Abbildung $\mathbf{F}_p^\times \overset{x \mapsto x^n}{\to} \mathbf{F}_p^\times$ hat $ggT(p-1, n)$ Elemente, da $\mathbf{F}_p^\times$ zyklisch ist. Daher gilt auch $\#\mathbf{F}_p^\times/\mathbf{F}_p^{\times n} = ggT(p-1, n)$. Damit erhält man

$$A = 2(p-2) + \left\{ \begin{array}{lll} 10 & \text{für} & p \equiv 1 \bmod 12 \\ 6 & \text{für} & p \equiv 5 \bmod 12 \\ 8 & \text{für} & p \equiv 7 \bmod 12 \\ 4 & \text{für} & p \equiv 11 \bmod 12 \end{array} \right\}$$

Wir wollen jetzt Morphismen zwischen elliptischen Kurven betrachten. Es gilt der wichtige Satz:

SATZ 49. *Seien (E_1, O_1) und (E_2, O_2) elliptische Kurven und $\phi : E_1 \to E_2$ ein nichtkonstanter Morphismus. Gilt $\phi(O_1) = O_2$, dann ist ϕ ein Gruppenhomomorphismus. Man nennt ϕ eine Isogenie und die Kurven E_1 und E_2 isogen.*

FOLGERUNG 20. *Sind (E_1, O_1) und (E_2, O_2) elliptische Kurven und $\phi : E_1 \to E_2$ ein nichtkonstanter Morphismus, dann gibt es eine Isogenie ψ und eine Translation τ mit $\phi = \tau \circ \psi$.*

Zum Beweis des Satzes brauchen wir ein Lemma:

LEMMA 11. *Sei $\phi : C_1 \to C_2$ ein nichtkonstanter Morphismus zwischen Kurven. Dann gilt*

$$\phi_*(Hauptdivisor) = Hauptdivisor.$$

Beweisskizze: Wir beschränken uns auf den Fall, daß $\overline{K}(C_1)$ über $\overline{K}(C_2)$ galoissch ist mit Galoisgruppe G. Dann operiert G auch auf C_1. Insbesondere gilt für jeden Punkt $P \in C_1$:

$$\phi^*\phi_* P = \sum_{\sigma \in G} \sigma P.$$

Sei $f \in \overline{K}(C_1)$ und $(f) = \sum_i n_i P_i$. Dann gilt

$$\begin{aligned} \phi^*\phi_*(div(f)) &= \phi^*\phi_*(\sum_i n_i P_i) = \sum_i \phi^*\phi_* P_i = \sum_i \sum_{\sigma \in G} \sigma P_i = \sum_{\sigma \in G} \sigma(\sum_i n_i P_i) = \\ &= \sum_{\sigma \in G} \sigma(f) = \sum_{\sigma \in G} (\sigma f) = div(\prod_{\sigma \in G} \sigma f). \end{aligned}$$

Nun ist aber $g = \prod_{\sigma \in G} \sigma f \in \overline{K}(C_2)$, also folgt $\phi^*\phi_*(div(f)) = \phi^*(div(g))$ und damit $\phi_*(div(f)) = div(g)$, also die Behauptung. ■

Beweis des Satzes: Zu zeigen ist für $P_1, P_2, P_3 \in E_1$:

$$P_1 \oplus P_2 = P_3 \quad \Rightarrow \quad \phi(P_1) \oplus \phi(P_2) = \phi(P_3).$$

Sei also $P_1 \oplus P_2 = P_3$. Dies bedeutet $P_1 + P_2 \sim P_3 + O_1$ und damit $P_1 + P_2 - P_3 - O_1 \sim 0$, d.h. $P_1 + P_2 - P_3 - O_1$ ist Hauptdivisor. Nach dem Lemma gilt dann

$$0 \sim \phi_*(P_1 + P_2 - P_3 - O_1) = \phi(P_1) + \phi(P_2) - \phi(P_3) - O_2,$$

was auf die gleiche Weise wieder $\phi(P_1) \oplus \phi(P_2) = \phi(P_3)$ liefert, also die Behauptung. ■

Ist A eine abelsche Gruppe, so bilden die Endomorphismen $\phi : A \to A$ einen Ring durch die Definitionen

$$\begin{aligned} 0(a) &= 0, \\ 1(a) &= id_A(a) = a, \\ (\phi_1 + \phi_2)(a) &= \phi_1(a) + \phi_2(a), \\ (\phi_1\phi_2)(a) &= \phi_1(\phi_2(a)). \end{aligned}$$

Dies überträgt sich sofort auf elliptische Kurven:

Definition 40. *Ist (E, O) eine elliptische Kurve, so ist*

$$End(E) = \{\phi : E \to E \text{ über } \overline{K} \text{ definierter Morphismus mit } \phi(O) = O\}$$

ein Ring, der sogenannte Endomorphismenring von E. Betrachtet man nur über K definierte Morphismen, so schreibt man $End_K(E)$. Die Einheitengruppe von $End(E)$

$$Aut(E) = \{\phi : E \to E \text{ Isomorphismus mit } \phi(O) = O\}$$

heißt die Automorphismengruppe von E.

Wir haben oben für Charakteristik $\neq 2, 3$ gesehen, daß jeder Isomorphismus $\phi : E \to E'$ zwischen elliptischen Kurven mit $\phi(O) = O'$ durch einen Koordinatenwechsel $x \mapsto u^2x, y \mapsto u^3y$, $u \in \overline{K}^\times$ gegeben ist. Wann liefert nun eine solche Transformation einen Automorphismus von E? Genau dann, wenn $(x, y) \mapsto (u^2x, u^3y)$ die Kurve E in sich überführt, d.h. die transformierte Gleichung muß identisch erfüllt sein, also:

$$u^6y^2 = u^6x^3 + au^2x + b \text{ bzw. } y^2 = x^3 + \frac{a}{u^4}x + \frac{b}{u^6},$$

was sofort die Bedingung $a = u^4a, b = u^6b$ liefert. Damit ergibt sich sofort folgender Satz:

Satz 50. *In Charakteristik $\neq 2, 3$ gilt für eine elliptische Kurve E:*

1. *Ist $j(E) \neq 0, 1728$, so ist*
$$Aut(E) = \{P \mapsto P, P \mapsto -P\} \simeq \mathbf{Z}/(2).$$
2. *Ist $j(E) = 1728$, so ist*
$$Aut(E) = \{(x, y) \mapsto (x, y), (x, y) \mapsto (-x, iy), (x, y) \mapsto (-x, -iy), (x, y) \mapsto (x, -y)\} \simeq \mathbf{Z}/(4).$$
3. *$j(E) = 0$, so ist*
$$Aut(E) = \{(x, y) \mapsto (x, \pm y), (x, y) \mapsto (\zeta_3 x, \pm y), (x, y) \mapsto (\zeta_3^2 x, \pm y)\} \simeq \mathbf{Z}/(6).$$

Aufgabe:

1. Zeige, daß die Kurve $y^2 = x^3 - x$ in Charakteristik 3 eine Automorphismengruppe der Ordnung 12 besitzt.
2. Zeige, daß $y^2 + y = x^3$ in Charakteristik 2 eine Automorphismengruppe der Ordnung 24 besitzt.

Die Bestimmung von $End(E)$ ist nicht so einfach. Ist E eine elliptische Kurve und $n \in \mathbf{Z}, n \geq 0$, so ist die Multiplikation mit n

$$E \to E, \quad P \mapsto nP = P + \cdots + P$$

eine Endomorpmismus, der manchmal mit $[n]$ bezeichnet wird. Entsprechend definiert man $[-n]$:

$$E \to E, \quad P \mapsto n(-P) = -P - \cdots - P.$$

Diese Endomorphismen hat man bei jeder elliptischen Kurve.

SATZ 51. *Sei (E, O) eine elliptische Kurve. Dann gilt:*

1. *$End(E)$ ist nullteilerfrei, d.h. $\phi\psi = 0$ impliziert $\phi = 0$ oder $\psi = 0$.*
2. *Die Abbildung*
$$\mathbf{Z} \to End(E), \quad n \mapsto [n]$$
ist ein injektiver Ringhomomorphismus. Also kann man immer $\mathbf{Z} \subseteq End(E)$ schreiben.

Beweis:

1. Sei $\phi\psi = 0$. Ein Morphismus $E \to E$ ist surjektiv oder konstant. Ist ψ surjektiv, so folgt $0 = \phi(\psi(E)) = \phi(E)$, also $\phi = 0$. Ist ψ konstant, so $\psi = 0$ wegen $\psi(O) = O$.
2. Wir beschränken uns auf elliptische Kurven der Form $y^2 = x^3 + ax + b$ in Charakteristik $\neq 2, 3$. Daß $[] : \mathbf{Z} \to End(E)$ ein Ringhomomorphismus ist, ist klar. Wir zeigen für jede Primzahl p, daß $[p] \neq 0$ gilt. Dann folgt nach 1. auch $[n] \neq 0$ für jede ganze Zahl $n \geq 0$.
1. Fall: $p = 2$: Sei $P = (x, y) \in E$ mit $y \neq 0$. Dann gilt $P \neq -P$, also $2P \neq 0$.
2. Fall: $p > 2$. Sei $e \in \overline{K}$ eine Nullstelle von $x^3 + ax + b$. Dann ist $P = (e, 0) \in E$ mit $P = -P$, also $2P = 0$. Es folgt mit $p = 2m + 1$:
$$pP = m(2P) + P = P \neq 0,$$
also die Behauptung. ■

Frage: Was kann man über die Struktur von $E(K)$ und $E(\overline{K})$ sagen?

DEFINITION 41. *Ist A eine abelsche Gruppe, so heißt für $n \in \mathbf{N}$*
$$A[n] = \{a \in A : na = 0\}$$
die n-Torsionsuntergruppe von A. Die Torsionselemente zusammen bilden die Torsionsuntergruppe von A:
$$A_{tor} = \cup_{n \geq 1} A[n].$$
Ist E eine elliptische Kurve, so heißt $E[n]$ auch die Untergruppe der n-Teilungspunkte von E.

Beispiel: $P = (x_0, y_0)$ auf E mit $y^2 = x^3 + ax + b$ hat genau dann Ordnung 2, wenn $(x_0, y_0) = P = -P = (x_0, -y_0)$, d.h. wenn $y_0 = 0$ gilt. Ist $x^3 + ax + b = (x - e_1)(x - e_1)(x - e_3)$, so sind also $(e_1, 0), (e_2, 0), (e_3, 0)$ genau die Punkte der Ordnung 2 und damit
$$E[2] = \{O, (e_1, 0), (e_2, 0), (e_3, 0)\} \simeq \mathbf{Z}/2 \oplus \mathbf{Z}/2.$$

Elliptische Kurven über $\mathbf{R}$

Wir betrachten E mit $y^2 = x^3 + ax + b$, $a, b \in \mathbf{R}$ und $\Delta = 4a^3 + 27b^2 \neq 0$. Es gibt zwei Fälle:

1. $x^3 + ax + b$ hat genau eine reelle Nullstelle, die andern beiden sind komplex konjugiert, also
$$x^3 + ax + b = (x - \alpha)(x + \frac{1}{2}\alpha + \beta i)(x + \frac{1}{2}\alpha - \beta i)$$
mit $\alpha, \beta \in \mathbf{R}, \beta \neq 0$, was durch Koeffizientenvergleich
$$a = -\frac{3}{4}\alpha^2 + \beta^2, \quad b = -\frac{1}{4}\alpha^3 - \alpha\beta^2$$
und damit
$$\Delta = \frac{1}{4}\beta^2(9\alpha^2 + 4\beta^2)^2 > 0$$
liefert. $E(\mathbf{R})$ ist zusammenhängend und es gilt $E(\mathbf{R}) \simeq \mathbf{R}/\mathbf{Z}$.
2. $x^3 + ax + b$ hat 3 reelle Nullstellen, also
$$x^3 + ax + b = (x - \alpha)(x - \beta)(x + \alpha + \beta),$$
was sofort
$$a = -\alpha^2 - \alpha\beta - \beta^2, \quad b = \alpha^2\beta + \alpha\beta^2$$
und damit
$$\Delta = -(\alpha + 2\beta)^2(2\alpha + \beta)^2(\alpha - \beta)^2 < 0$$
liefert. $E(\mathbf{R})$ hat zwei Zusammenhangskomponenten. Es gilt $E(\mathbf{R}) \simeq \mathbf{Z}/(2) \oplus \mathbf{R}/\mathbf{Z}$.

SATZ 52. *Ist E mit $y^2 = x^3 + ax + b$ eine elliptische Kurve über $\mathbf{R}$, so gilt*

$$E(\mathbf{R}) \simeq \left\{ \begin{array}{cc} \mathbf{R}/\mathbf{Z} & \textit{für } \Delta > 0 \\ \mathbf{Z}/(2) \oplus \mathbf{R}/\mathbf{Z} \; \textit{für } \Delta < 0 & \end{array} \right\}$$

Aufgabe: Bestimme die Struktur von $E(\mathbf{R})[n]$ für elliptische Kurven über $\mathbf{R}$.

Elliptische Kurven über $\mathbf{C}$ werden wir im nächsten Abschnitt behandeln.

Singuläre Weierstraßgleichungen

Was passiert mit unseren Additionsformeln, wenn E mit $y^2 = x^3 + ax + b$ singulär ist?

Ist $\Delta = 4a^3 + 27b^2 = 0$, so ist $(\frac{b}{2})^2 = (-\frac{a}{3})^3$, also gibt es wie üblich ein $c \in K$ mit $a = -3c^2, b = 2c^3$, d.h. die Kurve wird

$$E_c : y^2 = x^3 - 3c^2x + 2c^3.$$

Wegen $x^3 - 3c^2x + 2c^3 = (x-c)^2(x+2c)$ ist die Singularität in $S = (1 : c : 0)$.

Geometrische Überlegung: Eine Gerade durch S schneidet E_c höchstens noch in einem weiteren Punkt. Setzt man also $E_c^* = E_c \setminus \{S\}$, so liefert Tangenten- und Sekantenbildung für Punkte aus E_c^* wieder Punkte aus E_c^*, d.h. E_c^* ist abgeschlossen bzgl. der geometrischen Addition.

Algebraische Betrachtung: Setzt man $(y_0 : y_1 : y_2) = (1 : c : 0)$ in die Additionsformeln ein, so erhält man

$$(3c^3x_0^2 - 6c^2x_0x_1 + 3x_1^2 - x_2^2 : c(3c^3x_0^2 - 6c^2x_0x_1 + 3x_1^2 - x_2^2) : 0),$$

was für $(x_0 : x_1 : x_2) \neq (1 : c : 0)$ die Singularität ergibt, in der Singularität nicht definiert ist. (Also hat man auf E_c keine Gruppenstruktur mehr.) Wir betrachten jetzt zwei Fälle:

$\boxed{c = 0}$ Die Gleichung ist $y^2 = x^3$, die Zuordnung $(x, y) \mapsto \frac{x}{y} = s$ liefert dann eine Parametrisierung:

$$\phi : \mathbf{P}^1 \to E_0, (s_0 : s_1) \mapsto (s_1^3 : s_0^2s_1 : s_0^3).$$

Die Umkehrabbildung ist rational und durch $(x_0 : x_1 : x_2) \mapsto (x_2 : x_1)$ gegeben. Setzt man jetzt in die Formeln ein, so erhält man

$$\phi((1 : s)) + \phi((1 : t)) = ((s+t)^3 : s+t) : 1) = \phi((1 : s+t)).$$

Man erhält also einen Gruppenisomorphismus mit der additiven Gruppe des Grundkörpers:

$$E_0^* \simeq (\overline{K}, +).$$

Der Isomorphismus ist über K definiert.

$\boxed{c \neq 0}$ Die Tangenten in der Singularität sind $y = \pm\sqrt{3c}(x - c)$. Wir wählen $d \in K(\sqrt{3c})$ mit $3c = d^2$. Durch den Ansatz

$$t = \frac{y + \sqrt{3c}(x-c)}{y - \sqrt{3c}(x-c)}$$

erhalten wir eine Parametrisierung

$$x = \frac{d^2(t^2 + 10t + 1)}{3(t-1)^2}, \quad x = \frac{4d^3t(t+1)}{t-1)^3},$$

die wir mit ψ bezeichnen. Für $s, t \neq 0$ findet man

$$\psi((1 : s)) + \psi((1 : t)) = \psi((1 : st)).$$

Dies liefert also einen Isomorphismus von

$$E_c^* \simeq \overline{K}^\times.$$

Der Isomorphismus ist über $K(\sqrt{3c})$ definiert.

KAPITEL 9

Elliptische Kurven über C

Ist E eine über $\mathbf{C}$ definierte elliptische Kurve, so ist E auch eine Riemannsche Fläche, d.h. eine 1-dimensionale komplexe Mannigfaltigkeit. Es gibt auch einen wichtigen analytischen Aspekt elliptischer Kurven, der manchmal in der Funktionentheorie behandelt wird. Wir wollen hier ohne Beweise nur einige Grundtatsachen erwähnen.

Ein Gitter in $\mathbf{C}$ ist ein $\mathbf{Z}$-Modul

$$\Lambda = \mathbf{Z}\tau_1 + \mathbf{Z}\tau_2,$$

wo τ_1, τ_2 eine $\mathbf{R}$-Basis von $\mathbf{C}$ ist.
Eine Funktion f heißt periodisch bzgl. Λ, falls gilt

$$f(z+\tau) = f(z) \text{ für alle } \tau \in \Lambda,$$

was gleichwertig ist mit $f(z+\tau_1) = f(z+\tau_2) = f(z)$.

Welche Λ-periodischen Funktionen gibt es?
Der Satz von Liouville liefert sofort, daß nur die Konstanten holomorph und Λ-periodisch sind. Die wichtigste Λ-periodische Funktion ist die Weierstraßsche $\wp$-Funktion

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

$\wp(z)$ hat in allen $\omega \in \Lambda$ einen Pol zweiter Ordnung und ist sonst holomorph. Die Ableitung ist

$$\wp'(z) = \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{(z-\omega)^3}.$$

Definiert man

$$s_m = \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^m},$$

so erhält man für die Laurentreihenentwicklungen in $z=0$:

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + 3s_4z^2 + 5s_6z^4 + \cdots = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)s_{2n+2}z^{2n},\\
\wp'(z) &= -\frac{2}{z^3} + 6s_4z^2 + 20s_6z^3 + \ldots
\end{aligned}$$

Da es keine nichtkonstanten holomorphen Λ-periodischen Funktionen gibt, erhält man daraus schnell die Relation

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3 \quad \text{mit} \quad g_2 = 60s_4 \text{ und } g_3 = 140s_6.$$

Definiert man $E_\Lambda \subseteq \mathbf{P}^2$ durch $y^2 = 4x^3 - g_2x - g_3$, so induziert die Abbildung

$$z \mapsto (1 : \wp(z) : \wp'(z)) \text{ und } \omega \mapsto (0:0:1) \text{ für } \omega \in \Lambda$$

einen Isomorphismus

$$\mathbf{C}/\Lambda \simeq E_\Lambda$$

von komplexen Mannigfaltigkeiten, der auch ein Gruppenisomorphismus ist. Es gilt der wichtige Satz:

SATZ 53. *Jede elliptische Kurve über* $\mathbf{C}$ *ist als komplexe Mannigfaltigkeit und Gruppe (auf die eben beschriebene Weise) isomorph zu einer Riemannschen Fläche* $\mathbf{C}/\Lambda$*, wo* Λ *ein Gitter in* $\mathbf{C}$ *ist.*

Bemerkung: Ist $\Lambda = \mathbf{Z}\tau_1 + \mathbf{Z}\tau_2$ und $\tau = \frac{\tau_2}{\tau_1}$, so kann man durch Basiswechsel immer $Im(\tau) > 0$ erreichen. Definiert man nun

$$q = e^{2\pi i \tau}, \quad \sigma_k(n) = \sum_{d|n} d^k, \quad X = \sum_{n=1}^{\infty} \sigma_3(n) q^n, \quad Y = \sum_{n=1}^{\infty} \sigma_5(n) q^n,$$

so gilt

$$j = \frac{12(1+240X)^3}{5X + 1200X^2 + 96000X^3 + 7Y - 1764Y^2},$$

woraus man sofort die q-Entwicklung von j berechnen kann:

$$j = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \ldots$$

Die Koeffizienten dieser Entwicklung sind ganzzahlig.

Wir wollen jetzt die analytische Darstellung elliptischer Kurven anwenden.

Gruppenstruktur: Ist $\Lambda = \mathbf{Z}\tau_1 + \mathbf{Z}\tau_2$, so gilt als Gruppe

$$E = \mathbf{C}/\Lambda = (\mathbf{R}\tau_1 + \mathbf{R}\tau_2)/(\mathbf{Z}\tau_1 + \mathbf{Z}\tau_2) \simeq \mathbf{R}/Z \times \mathbf{R}/\mathbf{Z}.$$

Für die n-Torsionspunkte folgt damit

$$E[n] = (\mathbf{Z}\frac{1}{n}\tau_1 + \mathbf{Z}\frac{1}{n}\tau_2)/(\mathbf{Z}\tau_1 + \mathbf{Z}\tau_2) \simeq \frac{1}{n}\mathbf{Z}/\mathbf{Z} \times \frac{1}{n}\mathbf{Z}/\mathbf{Z} \simeq \mathbf{Z}/n \times \mathbf{Z}/n.$$

Eine andere Deutung ist folgende: Jeder Punkt von $\mathbf{C}/\Lambda$ wird durch einen Punkt aus

$$F = \{x\tau_1 + y\tau_2 : x, y \in \mathbf{R}, 0 \leq x, y < 1\}$$

repräsentiert. Wann liefert $z = x\tau_1 + y\tau_2 \in F$ einen n-Torsionspunkt? Genau dann, wenn $nz \in \Lambda$ gilt, d.h. für $nx, ny \in \mathbf{Z}$. Also werden die n-Teilungspunkte durch die Punkte

$$\frac{i}{n}\tau_1 + \frac{j}{n}\tau_2 : 0 \leq i, j < n$$

repräsentiert. Das sind n^2 und man sieht auch schnell

$$E[n] \simeq Z_n \times Z_n.$$

Bemerkung: Dieses Ergebnis gilt ähnlich auch für einen beliebigen Körper: Ist E eine elliptische Kurve über K und $ggT(n, char(K)) = 1$, so ist

$$E[n] \simeq \mathbf{Z}/n \times \mathbf{Z}/n.$$

Holomorphe Abbildungen: Sei

$$\phi : \mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$$

eine holomorphe Abbidung. Dies kann zu einer holomorphen Abbildung $f : \mathbf{C} \to \mathbf{C}$ geliftet werden, da $\mathbf{C}$ die universelle Überlagerung von $\mathbf{C}/\Lambda_2$ ist. Als Bedingung erhält man:

$$z_1 - z_2 \in \Lambda_1 \quad \Rightarrow \quad f(z_1) - f(z_2) \in \Lambda_2.$$

Für $\tau \in \Lambda_1$ ist also $f(z+\tau) - f(z) \in \Lambda_2$ für alle $z \in \mathbf{C}$, daher gibt es ein $c_\tau \in \Lambda_2$ mit

$$f(z+\tau) - f(z) = c_\tau.$$

Differenzieren liefert $f'(t+\tau) = f'(z)$. Also ist f' periodisch bzgl. Λ_1, also konstant. Daher ist

$$f(z) = \alpha z + \beta,$$

wozu man noch die Bedingung $\alpha\Lambda_1 \subseteq \Lambda_2$ hat. Daher folgt folgender Satz:

SATZ 54. *Die holomorphen Abbildungen $\mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$ werden durch lineare Abbildungen $\mathbf{C} \to \mathbf{C} : z \mapsto \alpha z + \beta$ induziert, für die $\alpha\Lambda_1 \subseteq \Lambda_2$ gilt.*

Man sieht hieran auch sofort, daß die Abbildungen, die 0 in 0 überführen, Gruppenhomomorphismen sind.

FOLGERUNG 21. *Für elliptische Kurven $\mathbf{C}/\Lambda$, $\mathbf{C}\Lambda'$ gilt:*

1. $\mathbf{C}/\Lambda \simeq \mathbf{C}/\Lambda' \quad \Longleftrightarrow \quad \alpha\Lambda = \Lambda'$ *für ein* $\alpha \in \mathbf{C}$.
2. $\mathbf{C}/\Lambda$ *ist isogen zu* $\mathbf{C}/\Lambda'$ *genau dann, wenn es ein* $\alpha \in \mathbf{C}, \alpha \neq 0$ *gibt mit* $\alpha\Lambda \subseteq \Lambda'$. *Insbesondere ist Isogenie auch eine Äquivalenzrelation.*
3. $End(E) = \{\alpha \in \mathbf{C} : \alpha\Lambda \subseteq \Lambda\}$. *(Insbesondere gilt* $\mathbf{Z} \subseteq End(E)$.*)*

Ist E eine elliptische Kurve über $\mathbf{C}$, so gibt es also ein Gitter Λ mit $E \simeq \mathbf{C}/\Lambda$. Wir wollen jetzt eine Normalform für Λ herleiten.
Wir nennen Gitter Λ_1 und Λ_2 ähnlich und schreiben $\Lambda_1 \sim \Lambda_2$, wenn $\mathbf{C}/\Lambda_1 \simeq \mathbf{C}/\Lambda_2$ gilt, was nach dem Satz gleichwertig ist mit: es gibt ein $\alpha \in \mathbf{C}$ mit $\alpha\Lambda_1 = \Lambda_2$.
Ist $\Lambda = \mathbf{Z}\tau_1 + \mathbf{Z}\tau_2$, so gilt

$$\Lambda = \mathbf{Z}\tau_1 + \mathbf{Z}\tau_2 \sim \mathbf{Z} + \mathbf{Z}\frac{\tau_2}{\tau_1} = \mathbf{Z} + \mathbf{Z}(-\frac{\tau_2}{\tau_1}),$$

also können wir $\Lambda = \mathbf{Z} + \mathbf{Z}\tau$ mit $Im(\tau) > 0$ erreichen, d.h. $\tau \in \mathfrak{H} = \{z \in \mathbf{C} : Im(z) > 0\}$ der oberen Halbebene von $\mathbf{C}$.

Satz 55. *Für* $\tau_1, \tau_2 \in \mathfrak{H}$ *gilt:*

$$\mathbf{Z} + \mathbf{Z}\tau_1 \sim \mathbf{Z} + \mathbf{Z}\tau_2 \quad \Longleftrightarrow \quad \text{es gibt } a, b, c, d \in \mathbf{Z} \text{ mit } ad - bc = 1 \text{ und } \tau_2 = \frac{a\tau_1 + b}{c\tau_2 + d}.$$

Die Bedingung an a, b, c, d *kann man auch als* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ *formulieren.*

Zum Beweis des Satzes brauchen wir noch eine Formel, die man schnell nachrechnet:

Lemma 12. *Für* $\tau \in \mathbf{C} \setminus \mathbf{R}$ *und* $a, b, c, d \in \mathbf{R}$ *gilt:*

$$Im(\frac{a\tau + b}{c\tau + d}) = \frac{(ad - bc)Im(\tau)}{|c\tau + d|^2}.$$

Beweis des Satzes:

- Die Gitter $\mathbf{Z} + \mathbf{Z}\tau_1$ und $\mathbf{Z} + \mathbf{Z}\tau_2$ seien ähnlich. Dann gibt es ein $\alpha \in \mathbf{C}$ mit
$$\mathbf{Z}\alpha + \mathbf{Z}\alpha\tau_2 = \alpha(\mathbf{Z} + \mathbf{Z}\tau_2) = \mathbf{Z} + \mathbf{Z}\tau_1.$$
$\alpha, \alpha\tau_2$ und $1, \tau_1$ sind nun $\mathbf{Z}$-Basen des gleichen Gitters, also gibt es $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{Z})$, d.h. $a, b, c, d \in \mathbf{Z}$ mit $ad - bc = \pm 1$ und
$$\begin{aligned} \alpha &= d + c\tau_1 \\ \alpha\tau_2 &= b + a\tau_1. \end{aligned}$$
Division ergibt
$$\tau_2 = \frac{a\tau_1 + b}{c\tau_1 + d}.$$
Für den Imaginärteil gilt
$$Im(\tau_2) = \frac{(ad - bc)Im(\tau_1)}{|c\tau_1 + d|^2},$$
also folgt wegen $Im(\tau_1), Im(\tau_2) > 0$ sofort $ad - bc > 0$ und damit $ad - bc = 1$.
- Die Umkehrung ist auch klar: Man wählt $\alpha = d + c\tau_1$ und liest alles rückwärts. ■

Bemerkung und Definition: Die Gruppe $G = SL_2(\mathbf{Z})/\{\pm 1\}$ operiert auf $\mathfrak{H}$ durch

$$SL_2(\mathbf{Z}) \times \mathfrak{H} \to \mathfrak{H}, \quad (\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tau) \mapsto \frac{a\tau + b}{c\tau + d}.$$

(Die Eigenschaften einer Gruppenoperation $(g_1 g_2)\tau = g_1(g_2\tau)$ und $1\tau = \tau$ rechnet man einfach nach.)
Die G-Bahn von τ ist

$$G\tau = \{\frac{a\tau + b}{c\tau + d} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G\}.$$

Zwei Gitter $\Lambda_1 = \mathbf{Z} + \mathbf{Z}\tau_1$ und $\Lambda_2 = \mathbf{Z} + \mathbf{Z}\tau_2$ sind also genau dann ähnlich, wenn τ_1 und τ_2 in der gleichen G-Bahn liegen. Wir wollen nun gewisse Elemente der Bahnen als Repräsentanten auszeichnen. Wir definieren

$$\begin{aligned}\mathfrak{F} &= \{\tau \in \mathfrak{H} : -\frac{1}{2} < Re(\tau) < \frac{1}{2}, |\tau| > 1\} \cup \\ &\cup \{\tau \in \mathfrak{H} : Re(\tau) = \frac{1}{2}, |\tau| > 1\} \cup \\ &\cup \{\tau \in \mathfrak{H} : 0 \leq Re(\tau) \leq \frac{1}{2}, |\tau| = 1\}.\end{aligned}$$

Dann gilt der

Satz 56. *Zu jedem Gitter Λ gibt es genau ein dazu ähnliches Gitter $\mathbf{Z}+\mathbf{Z}\tau$ mit $\tau \in \mathfrak{F}$. Anders formuliert: Zu jeder ellipitschen Kurve E gibt es genau ein $\tau \in \mathfrak{F}$ mit*

$$E \simeq \mathbf{C}/\mathbf{Z} + \mathbf{Z}\tau.$$

Beweis:

1. Wir geben zunächst ein konstruktives Verfahren an, wie man zu $\tau \in \mathfrak{H}$ einen Repräsentanten in $\mathfrak{F}$ findet.
   (a) In G gibt es die Elemente
   $$\tau \mapsto \tau + n \text{ für } n \in \mathbf{Z} \text{ und } \tau \mapsto -\frac{1}{\tau}.$$
   $\tau \mapsto \tau + n$ translatiert um $n \in \mathbf{Z}$, der Imaginärteil bleibt gleich. $\tau \mapsto -\frac{1}{\tau}$ ist in Polarkoordinaten $re^{i\varphi} \mapsto \frac{1}{r}e^{i(\pi-\varphi)}$, ist also eine Spiegelung am Einheitskreis und an der Geraden $Re(\tau) = 0$.
   (b) Es gilt
   $$Im(\tau + n) = Im(\tau) \quad \text{ und } \quad Im(-\frac{1}{\tau}) = \frac{Im(\tau)}{|\tau|^2}.$$
   (c) Sei jetzt $\tau \in \mathfrak{H}$.
   1. Schritt: Translatiere τ, so daß $-\frac{1}{2} < Re(\tau) \leq \frac{1}{2}$ gilt.
   2. Schritt: Ist $|\tau| \geq 1$, sind wir (fast) fertig. Sonst gehe über zu $-\frac{1}{\tau}$, das einen größeren Imaginärteil hat. Gehe dann zum 1. Schritt.
2. Wir wollen nun den Satz beweisen.
   (a) Sei $\tau \in \mathfrak{H}$. Gilt für $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ die Ungleichung $Im(A\tau) > Im(\tau)$, so folgt wegen $Im(A\tau)\frac{Im(\tau)}{|c\tau+d|^2}$
   $$1 > |c\tau + d|^2 = |(cx + d) + icy|^2 = (cx + d)^2 + c^2y^2.$$
   Man sieht, daß es nur endlich viele ganze Zahlen c, d mit $Im(A\tau) > Im(\tau)$ gibt. O.E. hat τ selbst schon maximalen Imaginärteil in der Bahn $G\tau$. Durch Translation können wir auch $-\frac{1}{2} < Re(\tau) \leq \frac{1}{2}$ erreichen.
   (b) Wegen $-\frac{1}{\tau} \in G\tau$ folgt also
   $$Im(-\frac{1}{\tau}) = \frac{Im(\tau)}{|\tau|^2} \leq Im(\tau)$$
   und daher auch $|\tau|^2 \geq 1$.
   (c) In den meisten Fällen gilt jetzt schon $\tau \in \mathfrak{F}$. Der einzige Ausnahmefall ist $|\tau| = 1$ und $-\frac{1}{2} < Re(\tau) < 0$. Dann ist aber $-\frac{1}{\tau} \in \mathfrak{F}$.
   (d) Wir wollen nun zeigen, daß jede Bahn $G\tau$ die Menge $\mathfrak{F}$ nur einmal schneidet. Sei $\tau, g\tau \in \mathfrak{F}$ für ein $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$. Indem wir eventuell statt τ und $g\tau$ das Paar $g^{-1}\tau$ und τ betrachten, können wir o.E. $Im(g\tau) \geq Im(\tau)$ annehmen. Dies liefert $|c\tau + d| \leq 1$.

(e) Sei $\tau = x + iy$. Dann gilt wegen $|x| \leq \frac{1}{2}$ und $x^2 + y^2 \geq 1$

$$\begin{aligned} 1 &\geq |c(x+iy)+d|^2 = c^2x^2 + 2xcd + d^2 + c^2y^2 = c^2(x^2+y^2) + 2xcd + d^2 \geq \\ &\geq c^2 - |c||d| + d^2 = (|c| - \frac{1}{2}|d|)^2 + \frac{3}{4}|d|^2 \end{aligned}$$

bzw. $(2|c| - |d|)^2 + 3|d|)^2 \leq 4$. Es gibt also wegen $ggT(c,d) = 1$ nur die Fälle ((c,d) und $(-c,-d)$ liefern das gleiche)

$$(c,d) \in \{(1,0),(0,1),(1,1),(1,-1)\}.$$

Fall $(c,d) = (1,0)$*:* Dann folgt $|\tau| = 1$ und $b = -1$, d.h. $g\tau = a - \frac{1}{\tau}$. Dies liefert weiter $a = 0$ und nach Wahl von $\mathbf{F}$ dann $\tau = i = -\frac{1}{\tau}$.
Fall $(c,d) = (0,1)$*:* Dann ist $a = 1$, $g\tau = \tau + b$, also $b = 0$.
Fall $(c,d) = (1,1)$*:* Aus obiger Abschätzung sieht man sofort, daß $x^2 + y^2 = 1$ und $x = -\frac{1}{2}$ gelten muß, was aber bei uns ausgeschlossen war.
Fall $(c,d) = (1,-1)$*:* Genau wie oben sieht man, daß $x^2 + y^2 = 1$ und $x = \frac{1}{2}$ gilt, also $\tau = \frac{1+\sqrt{-3}}{2}$. Für b folgt $b = -a - 1$ und damit

$$g\tau = \frac{a\tau - a - 1}{\tau - 1} = a - \frac{1}{\tau - 1} = a - \frac{1}{\zeta_3} = a + \tau,$$

was wieder $a = 0$, also nichts Neues ergibt. ∎

Komplexe Multiplikation

Wir haben für $E = \mathbf{C}/\Lambda$ gezeigt, daß

$$End(E) = \{\alpha \in \mathbf{C} : \alpha\Lambda \subseteq \Lambda\}$$

gilt. An dieser Darstellung sieht man sofort, daß $\mathbf{Z} \subseteq End(E)$ gilt. Gilt $\mathbf{Z} \neq End(E)$, so sagt man, E hat komplexe Multiplikation.
Sei jetzt $E \simeq \mathbf{C}/\Lambda$ gegeben mit $\Lambda = \mathbf{Z} + \mathbf{Z}\tau$, so daß $\mathbf{Z} \neq End(E)$ gilt.

1. Sei $\alpha \in \mathbf{C} \setminus \mathbf{Z}$ mit $\alpha\Lambda \subseteq \Lambda$. Dann gibt es $A, B, C, D \in \mathbf{Z}$ mit

$$\alpha = A + B\tau \quad \text{und} \quad \alpha\tau = C + D\tau.$$

2. Es folgt $C + D\tau = \alpha\tau = (A + B\tau)\tau$, also

$$B\tau^2 + (A - D)\tau - C = 0.$$

   Daher ist τ quadratisch über $\mathbf{Q}$. Da τ nicht reell ist, ist τ imaginärquadratisch, d.h. es gibt ein $d \geq 2$ quadratfrei mit

$$\tau \in \mathbf{Q}(\sqrt{-d}).$$

3. Wegen $\alpha = A + B\tau$ folgt sofort

$$\alpha \in \mathbf{Q}(\sqrt{-d}).$$

   Nun kann man das aber für jedes $\alpha \in End(E)$ machen. Also hat man

$$End(E) \subseteq \mathbf{Q}(\sqrt{-d}).$$

4. Schreiben wir obige Gleichung in Matrizenform

$$\alpha \begin{pmatrix} 1 \\ \tau \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} 1 \\ \tau \end{pmatrix} \quad \text{bzw.} \quad \begin{pmatrix} \alpha - A & -B \\ -C & \alpha - D \end{pmatrix} \begin{pmatrix} 1 \\ \tau \end{pmatrix} = 0,$$

   so ist die Determinante der Matrix 0, d.h.

$$\alpha^2 - (A + D)\alpha + (AD - BC) = 0.$$

   α genügt also einer Gleichung mit ganzzahligen Koeffizienten mit höchstem Koeffizienten 1, man sagt, α ist ganz über $\mathbf{Z}$.

Wir fassen dies zusammen:

Lemma 13. *Ist $\Lambda = \mathbf{Z} + \mathbf{Z}\tau$, $E = \mathbf{C}/\Lambda$ und $End(E) \neq \mathbf{Z}$, so gibt es eine quadratfreie ganze Zahl $d \geq 2$ mit*

$$\Lambda \subseteq \mathbf{Q}(\sqrt{-d})$$

und

$$End(E) \subseteq \{\alpha \in \mathbf{Q}(\sqrt{-d}) : \alpha \text{ ganz über } \mathbf{Z}\}.$$

Die in $\mathbf{Q}(\sqrt{-d})$ über $\mathbf{Z}$ ganzen Zahlen lassen sich nun leicht bestimmen:

Lemma 14. *Ist $d \geq 1$ quadratfrei und*

$$\omega = \omega_d = \left\{ \begin{array}{cc} \sqrt{-d} & \text{für } d \equiv 1,2 \bmod 4, \\ \frac{1+\sqrt{-d}}{2} & \text{für } d \equiv 3 \bmod 4, \end{array} \right\},$$

so gilt:

1. $\{\alpha \in \mathbf{Q}(\sqrt{-d}) : \alpha \text{ ganz über } \mathbf{Z}\} = \mathbf{Z}[\omega] = \mathbf{Z} + \mathbf{Z}\omega.$
2. *Ist $R \neq \mathbf{Z}$ ein Ring mit $R \subseteq \mathbf{Z}[\omega]$, so gibt es (genau) ein $f \in \mathbf{N}$ mit*

$$R = \mathbf{Z}[f\omega] = \mathbf{Z} + \mathbf{Z}f\omega.$$

f heißt der Führer von R.

Beweis:

1. (a) Wir zeigen zunächst $\subseteq$: Sei $\alpha \in \mathbf{Q}(\sqrt{-d})$ ganz über $\mathbf{Z}$, d.h. Nullstelle eines Polynoms $x^2 - Px + Q = 0$ mit $P, Q \in \mathbf{Z}$. Ist $\alpha \in \mathbf{Q}$, so überlegt man sich schnell, daß dann $r \in \mathbf{Z}$ gelten muß. Sei also $\alpha \notin \mathbf{Z}$. Schreiben wir

$$\alpha = r + s\sqrt{-d}, \quad \alpha' = r - s\sqrt{-d} \text{ mit } r, s \in \mathbf{Q},$$

so genügen sowohl α als auch α' der Gleichung $x^2 - Px + Q = 0$, also ist

$$x^2 - Px + Q = (x - \alpha)(x - \alpha')$$

und somit

$$\alpha + \alpha' = P \in \mathbf{Z} \text{ und } \alpha\alpha' = Q \in \mathbf{Z}.$$

Die erste Bedingung liefert $2r \in \mathbf{Z}$, also gibt es ein $k \in \mathbf{Z}$ mit $r = \frac{k}{2}$. Die zweite Bedingung liefert dann $\frac{k^2}{4} + s^2 d \in \mathbf{Z}$, also insbesondere $4s^2 d = (2s)^2 d \in \mathbf{Z}$. Da d quadratfrei ist, folgt $2s \in \mathbf{Z}$, also gibt es $\ell \in \mathbf{Z}$ mit $s = \frac{\ell}{2}$, d.h.

$$\alpha = \frac{k + \ell\sqrt{-d}}{2} \quad \text{mit} \quad k, \ell \in \mathbf{Z}.$$

In dieser Form gilt

$$\alpha\alpha' = \frac{k^2 + d\ell^2}{4} \in \mathbf{Z}, \text{ also } k^2 + d\ell^2 \equiv 0 \bmod 4.$$

Nun sind nur 0 und 1 Quadrate modulo 4.

1. Fall: $d \equiv 1,2 \bmod 4$: Dann ist $k \equiv \ell \equiv 0 \bmod 2$ und somit

$$\alpha \in \mathbf{Z} + \mathbf{Z}\sqrt{-d} = \mathbf{Z}[\sqrt{-d}].$$

2. Fall: $d \equiv 3 \bmod 4$: Dann ist $k \equiv \ell \equiv 0 \bmod 2$ oder $k \equiv \ell \equiv 1 \bmod 2$, also

$$\alpha \in \mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{-d}}{2} = \mathbf{Z}[\frac{1+\sqrt{-d}}{2}].$$

(Daß die entsprechenden Gleichheiten gelten, muß man natürlich noch überprüfen.)

(b) $\supseteq$: Übung.

2. Setzt man

$$f = ggT(b \in \mathbf{Z} : a + b\omega \in R),$$

so zeigt man leicht $R = \mathbf{Z}[f\omega]$. ∎

Überlegung: Sei $d \geq 2$ quadratfrei und $\tau = \frac{a+b\sqrt{-d}}{c}$ mit $ggT(a,b,c) = 1$ und $b, c \geq 1$. Sei $\Lambda = \mathbf{Z} + \mathbf{Z}\tau$. Wir wollen $End(\mathbf{C}/\Lambda)$ bestimmen.

- $\boxed{d \equiv 1,2 \bmod 4}$ Wir überlegen, wann $\mathbf{Z}[f\sqrt{-d}] \subseteq End(E)$ gilt, was äquivalent ist mit $f\sqrt{-d}\Lambda \subseteq \Lambda$.
  1. Es gibt $A, B, C, D \in \mathbf{Q}$ mit
  $$f\sqrt{-d} = A + B\tau \quad \text{und} \quad f\sqrt{-d}\tau = C + D\tau.$$
  Durch Koeffizientenvergleich findet man
  $$A = -\frac{af}{b}, \quad B = \frac{cf}{b}, \quad C = -\frac{(a^2+db^2)f}{bc}, \quad D = \frac{af}{b}.$$
  2. Wir nehmen jetzt an, es gilt $A, B, C, D \in \mathbf{Z}$. Dann folgt $b|af$ und $b|cf$, also $b|f$. Wir schreiben $f = bk$ mit $k \in \mathbf{Z}$. Es bleibt nur eine Bedingung, nämlich $bc|(a^2+db^2)f$, was sich jetzt in $c|(a^2+db^2)k$ übersetzt. Dies ist aber äquivalent mit
  $$\frac{c}{ggT(c, a^2+db^2)}|k, \text{ d.h. } k = \frac{c}{ggT(c, a^2+db^2)}\ell \text{ für ein } \ell \in \mathbf{Z}.$$
  Also hat man
  $$f = \frac{bc}{ggT(c, a^2+db^2)}\ell.$$
  3. Diese Form von f ist auch hinreichend für $A, B, C, D \in \mathbf{Z}$.
  4. Daher folgt
  $$End(E) = \mathbf{Z}[\frac{bc}{ggT(c, a^2+db^2)}\sqrt{-d}].$$
- $\boxed{d \equiv 3 \bmod 4}$ Wir überlegen, wann $\mathbf{Z}[f\frac{1+\sqrt{-d}}{2}] \subseteq End(E)$ gilt, was äquivalent ist mit $f\frac{1+\sqrt{-d}}{2}\Lambda \subseteq \Lambda$.
  1. Wir haben die Gleichungen
  $$f\frac{1+\sqrt{-d}}{2} = A + B\tau, \quad f\frac{1+\sqrt{-d}}{2}\tau = C + D\tau$$
  mit
  $$A = \frac{(b-a)f}{2b}, \quad B = \frac{cf}{2b}, \quad C = -\frac{(a^2+db^2)f}{2bc}, \quad D = \frac{(a+b)f}{2b},$$
  woraus sich zusätzlich
  $$A + D = f \text{ und } A - D = -\frac{af}{b}$$
  ergibt.
  2. Wir nehmen jetzt an, daß $A, B, C, D \in \mathbf{Z}$ gilt. Dann gilt $b|af$ und $b|cf$, also $b|f$. Wir schreiben $f = bk$ für ein $k \in \mathbf{Z}$. Es gilt dann
  $$A = \frac{(b-a)k}{2}, \quad B = \frac{ck}{2}, \quad C = -\frac{(a^2+db^2)k}{2c}, \quad D = \frac{(a+b)k}{2}.$$
  3. Aus C erhält man
  $$2c|(a^2+db^2)k, \text{ also } \frac{2c}{ggT(2c, a^2+db^2)}|k,$$
  so daß es ein $\ell \in \mathbf{Z}$ gibt mit
  $$k = \frac{2c}{ggT(2c, a^2+db^2)}\ell,$$
  was wiederum sofort
  $$f = \frac{2bc}{ggT(2c, a^2+db^2)}\ell$$
  liefert.
  4. Die verbleibenden Bedingungen lauten jetzt
  $$(b-a)\frac{2c}{ggT(2c, a^2+db^2)}\ell \equiv 0 \bmod 2 \text{ und } c\frac{2c}{ggT(2c, a^2+db^2)}\ell \equiv 0 \bmod 2.$$
  5. Man zeige jetzt: Gilt $a \equiv b \bmod 2$ und $c \equiv 1 \bmod 2$, so braucht man noch $\ell \equiv 0 \bmod 2$, in den anderen Fällen sind die Bedingungen erfüllt.

6. Damit erhält man jetzt
$$End(E) = \mathbf{Z}[f\frac{1+\sqrt{-d}}{2}]$$
mit
$$\left\{\begin{array}{ll} f = \frac{4bc}{ggT(2c,a^2+db^2)} & \text{für } a \equiv b \bmod 2 \text{ und } c \equiv 1 \bmod 2, \\ f = \frac{2bc}{ggT(2c,a^2+db^2)} & \text{sonst.} \end{array}\right\}$$

Wir fassen das Ergebnis zusammen:

Satz 57. *Sei $d \geq 1$ quadratfrei. Sind $a, b, c \in \mathbf{Z}$ mit $ggT(a, b, c) = 1$, $b, c \geq 1$, $\tau = \frac{a+b\sqrt{-d}}{c}$ und setzt man*
$$\begin{aligned} f &= \frac{bc}{ggT(c, a^2+db^2)} && \textit{im Fall } d \equiv 1 \textit{ oder } 2 \bmod 4, \\ f &= \frac{2bc}{ggT(2c, a^2+db^2)} && \textit{im Fall } d \equiv 3 \bmod 4 \textit{ und } a \not\equiv b \bmod 2 \textit{ oder } c \equiv 0 \bmod 2, \\ f &= \frac{4bc}{ggT(2c, a^2+db^2)} && \textit{im Fall } d \equiv 3 \bmod 4 \textit{ und } a \equiv b \bmod 2 \textit{ und } c \equiv 1 \bmod 2, \end{aligned}$$
so gilt
$$End(\mathbf{C}/\mathbf{Z}+\mathbf{Z}\tau) = \mathbf{Z}[f\omega_d].$$

Haben wir also eine elliptische Kurve in der Form $E = \mathbf{C}/\mathbf{Z}+\mathbf{Z}\tau$ gegeben, so können wir $End(E)$ berechnen. Wir interessieren uns jetzt für die Umkehrung.

Frage: Welche elliptischen Kurven haben den Endomorphismenring Ring $\mathbf{Z}[f\omega_d]$?

- Sei $E = \mathbf{C}/\mathbf{Z}+\mathbf{Z}\tau$ mit $End(E) = \mathbf{Z}[f\omega_d]$ und $\tau \in \mathfrak{F}$. Wir schreiben $\tau = \frac{a+b\sqrt{-d}}{c}$ mit $ggT(a, b, c) = 1$ und $b, c \geq 1$ und erhalten aus $\tau \in \mathfrak{F}$ insbesondere $|a| \leq \frac{1}{2}c$ und $c \leq \sqrt{a^2+db^2}$. Schreibt man dies $4a^2 \leq c^2$ und $c^2 \leq a^2+db^2$, so folgt sofort $3a^2 \leq db^2$, also $|a| \leq \sqrt{\frac{d}{3}}b$. Aus den Formeln des gerade bewiesenen Satzes sieht man sofort $b|f$. Wir fassen diese Ungleichungen nochmals zusammen:
$$b|f, \quad |a| \leq \sqrt{\frac{d}{3}}b, \quad 2|a| \leq c \leq \sqrt{a^2+db^2}.$$
Man sieht sofort, daß bei vorgegebenem d und f nur endlich viele Möglichkeiten für a, b, c existieren.
- Ist $|\tau| = 1$, also $c^2 = a^2+db^2$, so muß auch $a \geq 0$ gelten. Ist $|a| = \frac{1}{2}c$, so muß $a \geq 0$ gelten.
- Man überlegt sich sofort, daß ein τ, das diesen Ungleichungen genügt, auch wirklich in $\mathfrak{F}$ liegt.
- Jetzt muß man nur noch testen, ob τ wirklich Führer f hat.

Damit haben wir bewiesen:

Satz 58. *Sei $d \geq 1$ quadratfrei und $f \geq 1$. Sei $C(d, f)$ die Menge aller Tripel (a, b, c) mit folgenden Eigenschaften:*

- $a \in \mathbf{Z}$, $b, c \in \mathbf{N}$, $ggT(a, b, c) = 1$
- $$b|f, \quad |a| \leq \sqrt{\frac{db^2}{3}}, \quad 2|a| \leq c \leq \sqrt{a^2+db^2}$$
- *Gilt $c^2 = a^2+db^2$ oder $2|a| = c$, so gilt $a \geq 0$.*
- *a, b, c, d, f erfüllen die entsprechende Formel des letzten Satzes.*

Dann sind $\mathbf{C}/(\mathbf{Z}+\mathbf{Z}\frac{a+b\sqrt{-d}}{c})$, $(a, b, c) \in C(d, f)$, genau die elliptischen Kurven mit Endomorphismenring $\mathbf{Z}[f\omega_d]$. Insbesondere gibt es nur endlich viele davon. Die Zahl $\#C(d, f)$ heißt auch die Klassenzahl von $\mathbf{Z}[f\omega_d]$.

Wir haben damit praktisch einen Algorithmus beschrieben, wie man alle elliptischen Kurven mit vorgegebenem Endomorphismenring ($\neq \mathbf{Z}$) findet.

Algorithmus: d und f seien gegeben.

- $b \geq 1$ durchlaufe alle Teiler von f.

- a laufe von 0 bis $\sqrt{\frac{db^2}{3}}$.
- c durchlaufe den Bereich $2a \leq c \leq \sqrt{a^2 + db^2}$.
- Teste, ob $ggT(a, b, c) = 1$ gilt.
- Teste, ob τ den Führer f hat. Wenn ja, drucke (a, b, c) aus. Ist $2a < c$, $c^2 < a^2 + db^2$ und $a > 0$, so drucke auch $(-a, b, c)$ aus.
- Nächstes c, nächstes a, nächtes b.

Beispiel: $d = 1, f = 3$. Wir finden $C(1, 3) = \{(0, 3, 1), (1, 3, 2)\}$, der Ring $\mathbf{Z}[3i]$ hat also Klassenzahl 2.

Bemerkung: Es ist (seit Gauß) ein bekanntes (nichttriviales) Problem in der Zahlentheorie, alle Ringe mit vorgegebener Klassenzahl zu finden. Es gibt 13 Ringe mit Klassenzahl 1.

Hat E komplexe Multiplikation, so ist also $End(E) = \mathbf{Z}[f\omega_d]$ und $E = \mathbf{C}/\mathbf{Z} + \mathbf{Z}\tau$ für ein $\tau \in \mathbf{Q}(\sqrt{-d})$. Was kann man über die j-Invariante bzw. die Gleichung von E sagen? Hier gilt der wichtige

SATZ 59. *Sei $\mathbf{Z}[f\omega_d]$ gegeben und $E_i = \mathbf{C}/\mathbf{Z} + \mathbf{Z}\tau_i$, $i = 1, \ldots, h$ die elliptischen Kurven mit Endomorphismenring $\mathbf{Z}[f\omega_d]$. Dann ist*

$$H_{d,f}(x) = \prod_{i=1}^{h} (x - j(\tau_i))$$

ein irreduzibles Polynom in $\mathbf{Z}[x]$. Die $j(E_i)$'s sind also (ganz) algebraisch vom Grad h und konjugiert zueinander.

Beweisansatz: Wir können den Satz nicht vollständig beweisen. Sei $j_i = j(E_i) = j(\tau_i)$. Wir wählen eine Gleichung $y^2 = x^3 + a_i x + b_i$ für E_i. Sei σ ein Körperautomorphismus von $\mathbf{C}$. Dann hat auch $\sigma(E_i) : y^2 = x^3 + \sigma(a_i)x + \sigma(b_i)$ Endomorphismenring $\mathbf{Z}[f\sqrt{-d}]$. Also ist $\sigma(j_i) \in \{j_1, \ldots, j_h\}$. D.h. die Menge

$$\{j_1, \ldots, j_h\}$$

ist invariant unter allen Automorphismen von $\mathbf{C}$. Folglich hat

$$\prod_{i=1}^{h} (x - j_i)$$

Koeffizienten in $\mathbf{Q}$. ■

Ist $y^2 = x^3 + ax + b$ eine Gleichung für E mit j-Invariante j, so ist $\mathbf{Q}(j) \subseteq \mathbf{Q}(a, b)$. Außerdem können wir a und b so wählen, daß gilt $\mathbf{Q}(a, b) = \mathbf{Q}(j)$. Damit folgt dann:

FOLGERUNG 22. *Hat E Endomorphismenring $\mathbf{Z}[f\omega_d]$ und $\mathbf{Z}[f\omega_d]$ Klassenzahl h, so kann E über einem Körper vom Grad h definiert werden, aber nicht über einem Körper kleineren Grades.*

Ist die Klassenzahl 1, so ist also $j \in \mathbf{Z}$. Die Tabelle gibt alle Ringe $\mathbf{Z}[f\omega]$ mit Klassenzahl 1 an und listet zugehörige j-Invarianten und Beispiele für zugehörige Kurven auf.

Tabelle der singulären rationalen j-Invarianten

Ring	j	Beispiel
$\mathbf{Z}[\sqrt{-1}]$	$2^6 \cdot 3^3$	$y^2 = x^3 - x$
$\mathbf{Z}[2\sqrt{-1}]$	$2^3 \cdot 3^3 \cdot 11^3$	$y^2 = x^3 - 11x - 14$
$\mathbf{Z}[\sqrt{-2}]$	$2^6 \cdot 5^3$	$y^2 = x^3 - 30x - 56$
$\mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$	0	$y^2 = x^3 - 1$
$\mathbf{Z}[\sqrt{-3}]$	$2^4 \cdot 3^3 \cdot 5^3$	$y^2 = x^3 - 15x - 22$
$\mathbf{Z}[\frac{1+3\sqrt{-3}}{2}]$	$-2^{15} \cdot 3 \cdot 5^3$	$y^2 = x^3 - 120x - 506$
$\mathbf{Z}[\frac{1+\sqrt{-7}}{2}]$	$-3^3 \cdot 5^3$	$y^2 = x^3 - 35x - 98$
$\mathbf{Z}[\sqrt{-7}]$	$3^3 \cdot 5^3 \cdot 17^3$	$y^2 = x^3 - 595x - 5586$
$\mathbf{Z}[\frac{1+\sqrt{-11}}{2}]$	-2^{15}	$y^2 = x^3 - 264x - 1694$
$\mathbf{Z}[\frac{1+\sqrt{-19}}{2}]$	$-2^{15} \cdot 3^3$	$y^2 = x^3 - 152x - 722$
$\mathbf{Z}[\frac{1+\sqrt{-43}}{2}]$	$-2^{18} \cdot 3^3 \cdot 5^3$	$y^2 = x^3 - 3440x - 77658$
$\mathbf{Z}[\frac{1+\sqrt{-67}}{2}]$	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	$y^2 = x^3 - 29480x - 1948226$
$\mathbf{Z}[\frac{1+\sqrt{-163}}{2}]$	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	$y^2 = x^3 - 8697680x - 9873093538$

Ist die Klassenzahl von $\mathbf{Z}[f\omega_d]$ gleich 2, so sind die zugehörigen j-Invarianten quadratisch über $\mathbf{Q}$.

Beispiel: Wir betrachten $\mathbf{Z}[3i]$ mit der Klassenzahl 2. Die elliptischen Kurven mit Endomorphismenring $\mathbf{Z}[3i]$ sind $E_k = \mathbf{C}/\mathbf{Z} + \mathbf{Z}\tau_k$, wo

$$\tau_1 = 3i \quad \text{und } \tau_2 = \frac{1+3i}{2}$$

ist. Dann ist

$$q_1 = e^{2\pi i \tau_1} = e^{-6\pi} \approx 0.65 \cdot 10^{-8}, \quad q_2 = e^{2\pi i \tau_2} = -e^{-3\pi} \approx -0.81 \cdot 10^{-4}$$

und

$$j_1 \approx 0.15 \cdot 10^9 + 744 + 0.0013 + 0.91 \cdot 10^{-9} + 0.24 \cdot 10^{-15},$$
$$j_2 \approx -1.24 \cdot 10^5 + 744 - 15.89 + 0.14 - 0.00045 + 0.86 \cdot 10^{-6} - 0.11 \cdot 10^{-8} + 0.12 \cdot 10^{-12}.$$

Daraus schließt man dann,

$$j_1 + j_2 = 153542016 \text{ und } j_1 j_2 = -1790957481984,$$

woraus sich sofort

$$j_{1/2} = 767710008 \pm 44330496\sqrt{3}$$

ergibt.

Die folgende Tabelle gibt sämtliche Ringe mit Klassenzahl 2 an und die zugehörigen j-Invarianten.

Ringe mit Klassenzahl 2 und zugehörige j-Invariante

d	f	j
1	3	$76771008 \pm 44330496\sqrt{3}$
1	4	$41113158120 \pm 29071392966\sqrt{2}$
1	5	$22015749613248 \pm 9845745509376\sqrt{5}$
2	2	$26125000 \pm 18473000\sqrt{2}$
2	3	$188837384000 \pm 77092288000\sqrt{6}$
3	4	$1417905000 \pm 818626500\sqrt{3}$
3	5	$-327201914880 \pm 146329141248\sqrt{5}$
3	7	$-17424252776448000 \pm 3802283679744000\sqrt{21}$
5	1	$632000 \pm 282880\sqrt{5}$
6	1	$2417472 \pm 1707264\sqrt{2}$
7	4	$137458661985000 \pm 51954490735875\sqrt{7}$
10	1	$212846400 \pm 95178240\sqrt{5}$
11	3	$-18808030478336 \pm 3274057859072\sqrt{33}$
13	1	$3448440000 \pm 956448000\sqrt{13}$
15	1	$-191025/2 \pm 85995/2\sqrt{5}$
15	2	$37018076625/2 \pm 16554983445/2\sqrt{5}$
22	1	$3147421320000 \pm 2225561184000\sqrt{2}$
35	1	$-58982400 \pm 26378240\sqrt{5}$
37	1	$19830091900536000 \pm 3260047059360000\sqrt{37}$
51	1	$-2770550784 \pm 671956992\sqrt{17}$
58	1	$302364978924945672000 \pm 56147767009798464000\sqrt{29}$
91	1	$-5179536506880 \pm 1436544958464\sqrt{13}$
115	1	$-213932305612800 \pm 95673435586560\sqrt{5}$
123	1	$-677073420288000 \pm 105741103104000\sqrt{41}$
187	1	$-2272668190894080000 \pm 551203000178688000\sqrt{17}$
235	1	$-411588709724712960000 \pm 184068066743177379840\sqrt{5}$
267	1	$-98415459270397440000000 \pm 10432017818647326720000\sqrt{89}$
403	1	$-1226405694614665695989760000 \pm 340143739727246741938176000\sqrt{13}$
427	1	$-7805727756261891959906304000 \pm 999421027517377348595712000\sqrt{61}$

Das MAPLE-Programm cl

```
# Das Programm C berechnet zu vorgegebenem d und f alle elliptischen
# Kurven mit Endomorphismenring Z[f*omega_d], gegeben durch [a,b,c]
# tau=(a+b*sqrt(-d))c.
#
# Das Programm h berechnet die Klassenzahl.
#
# Das Programm F berechnet f"ur tau=(a+b*sqrt(-d))c den F"uhrer f
# des Ringes End(C/(Z+Z*tau)).

F:=proc(a,b,c,d)
ff:=0;
if d mod 4=1 or d mod 4=2 then ff:=b*c/igcd(c,a^2+d*b^2);fi;
if d mod 4=3 then ff:=2*b*c/igcd(2*c,a^2+d*b^2);
   if (a-b) mod 2=0 and c mod 2=1 then ff:=ff*2;fi;
fi;
ff;
end;

C:=proc(d,f)
for b from 1 to f do
if f mod b=0 then
   for a from 0 to trunc(sqrt(d/3)*b) do
   for c from 2*a to trunc(sqrt(a^2+d*b^2)) do
   if igcd(a,b,c)=1 then
      if f=F(a,b,c,d) then print([a,b,c]);
         if 2*a<c and c^2<a^2+d*b^2 and a>0 then print([-a,b,c]);fi;
      fi;
   fi;
   od;
   od;
fi;
od;
end;

h:=proc(d,f)
H:=0;
for b from 1 to f do
if f mod b=0 then
   for a from 0 to trunc(sqrt(d/3)*b) do
   for c from 2*a to trunc(sqrt(a^2+d*b^2)) do
   if igcd(a,b,c)=1 then
      if f=F(a,b,c,d) then H:=H+1;
         if 2*a<c and c^2<a^2+d*b^2 and a>0 then H:=H+1;fi;
      fi;
   fi;
   od;
   od;
fi;
od;
H;
end;
```

UBASIC-Programme cl.ub und clh.ub

```
10   input "d,f=";D,F
20   for B=1 to F:if F@B<>0 then goto 90
30   for A=0 to isqrt(D*B^2/3)
40   for C=2*A to isqrt(A^2+D*B^2):if gcd(A,B,C)>1 then goto 70
50   if fnF(A,B,C)=F then print A;B;C
60   if fnF(A,B,C)=F and 2*A<C and C^2<A^2+D*B^2 and A>0 then print -A;B;C
70   next C
80   next A
90   next B
100  goto 10
110  fnF(Aa,Bb,Cc)
120  Ff=0
130  if D@4=1 or D@4=2 then Ff=Bb*Cc\gcd(Cc,Aa^2+D*Bb^2)
140  if D@4=3 then Ff=2*Bb*Cc\gcd(2*Cc,Aa^2+D*Bb^2)
150  if D@4=3 and (A-B)@2=0 and C@2=1 then Ff=Ff*2
160  return(Ff)
```

```
10   input "d,f=";D,F:H=0
20   for B=1 to F:if F@B<>0 then goto 90
30   for A=0 to isqrt(D*B^2/3)
40   for C=2*A to isqrt(A^2+D*B^2):if gcd(A,B,C)>1 then goto 70
50   if fnF(A,B,C)=F then H=H+1
60   if fnF(A,B,C)=F and 2*A<C and C^2<A^2+D*B^2 and A>0 then H=H+1
70   next C
80   next A
90   next B
100  print "h=";H:goto 10
110  fnF(Aa,Bb,Cc)
120  Ff=0
130  if D@4=1 or D@4=2 then Ff=Bb*Cc\gcd(Cc,Aa^2+D*Bb^2)
140  if D@4=3 then Ff=2*Bb*Cc\gcd(2*Cc,Aa^2+D*Bb^2)
150  if D@4=3 and (A-B)@2=0 and C@2=1 then Ff=Ff*2
160  return(Ff)
```

Klassenzahlen $h = 3$ für $1 \le d \le 200$ und $1 \le f \le 10$

```
d= 3 f= 6 h= 3
d= 3 f= 9 h= 3
d= 11 f= 2 h= 3
d= 19 f= 2 h= 3
d= 23 f= 1 h= 3
d= 23 f= 2 h= 3
d= 31 f= 1 h= 3
d= 31 f= 2 h= 3
d= 43 f= 2 h= 3
d= 59 f= 1 h= 3
d= 67 f= 2 h= 3
d= 83 f= 1 h= 3
d= 107 f= 1 h= 3
d= 139 f= 1 h= 3
d= 163 f= 2 h= 3
```

Klassenzahl 2 und $1 \le d \le 500$, $1 \le f \le 10$

d	f	$(a_1, b_1, c_1), (a_2, b_2, c_2)$
1	3	$(0,3,1),(1,3,2)$
1	4	$(1,2,2),(0,4,1)$
1	5	$(0,5,1),(1,5,2)$
2	2	$(0,2,1),(1,2,3)$
2	3	$(0,3,1),(0,3,2)$
3	4	$(0,2,1),(0,2,3)$
3	5	$(1,5,2),(3,5,6)$
3	7	$(1,7,2),(3,7,6)$
5	1	$(0,1,1),(1,1,2)$
6	1	$(0,1,1),(0,1,2)$
7	4	$(0,1,2),(0,2,1)$
10	1	$(0,1,1),(0,1,2)$
11	3	$(1,3,2),(1,3,10)$
13	1	$(0,1,1),(1,1,2)$
15	1	$(1,1,2),(1,1,4)$
15	2	$(0,1,1),(0,1,3)$
22	1	$(0,1,1),(0,1,2)$
35	1	$(1,1,2),(1,1,6)$
37	1	$(0,1,1),(1,1,2)$
51	1	$(1,1,2),(3,1,6)$
58	1	$(0,1,1),(0,1,2)$
91	1	$(1,1,2),(3,1,10)$
115	1	$(1,1,2),(5,1,10)$
123	1	$(1,1,2),(3,1,6)$
187	1	$(1,1,2),(3,1,14)$
235	1	$(1,1,2),(5,1,10)$
267	1	$(1,1,2),(3,1,6)$
403	1	$(1,1,2),(9,1,22)$
427	1	$(1,1,2),(7,1,14)$

Vergleich von $h_{d,f}$ und $h_{d,1}$
Es gilt der Satz

Satz 60.

$$h_{d,f} = h_{d,1} \frac{f}{[\mathbf{Z}[\omega]^\times : \mathbf{Z}[f\omega]^\times]} \prod_{p|f} (1 - \left(\frac{D}{p}\right) \frac{1}{p}),$$

wo D *die Diskriminante und* $\left(\frac{D}{p}\right)$ *das Kroneckersymbol bezeichnet.*

KAPITEL 10

Elliptische Kurven über Q

Uns interessiert vor allem die Gruppe der $\mathbf{Q}$-rationalen Punkte $E(\mathbf{Q})$ auf einer über $\mathbf{Q}$ definierten elliptischen Kurve E.

Als Beispiel werden wir folgendes betrachten:

Beispiel: Sei E definiert durch $y^2 = x^3 - 25x$. Alle 2-Teilungspunkte sind über $\mathbf{Q}$ definiert: $(0,0), (5,0), (-5,0)$. Mit dem Computer findet man folgende Punkte mit Höhe ≤ 100:

$$(0:0:1) = O, \quad (1:0:0) = (0,0), \quad (1:5:0) = (5,0), \quad (1:-5:0) = (-5,0),$$
$$(1:-4:\pm 6) = (-4, \pm 6), \quad (8:50:\pm 75) = (\frac{25}{4}, \pm\frac{75}{8}),$$
$$(27:-15:\pm 100) = (-\frac{5}{9}, \pm\frac{100}{27}), \quad (1:45:\pm 300) = (45, \pm 300)$$

Ohne Beweis erwähnen wir folgenden wichtigen Satz:

SATZ 61 (Siegel). *Ist $y^2 = x^3 + ax + b$ mit $a, b \in \mathbf{Z}$ eine elliptische Kurve, so gibt es nur endlich viele Lösungen $x, y \in \mathbf{Z}$.*

Aus dem Beispiel kann man noch etwas über die Nenner rationaler Punkte erahnen:

LEMMA 15. *Sei $y^2 = x^3 + ax + b$ mit $a, b \in \mathbf{Z}$ eine elliptische Kurve E. Jeder Punkt $P \in E(\mathbf{Q})$, $P \neq O$ hat dann die Gestalt*

$$P = (\frac{r}{m^2}, \frac{s}{m^3}) \quad \text{mit } m \in \mathbf{N}, r, s \in \mathbf{Z}, \quad ggT(r,m) = ggT(s,m) = 1.$$

Beweis: Wir setzen an $P = (\frac{r}{k}, \frac{s}{\ell})$ mit $ggT(r,k) = ggT(s,\ell) = 1$. Einsetzen ergibt:

$$s^2 \cdot k^3 = (r^3 + ark^2 + bk^3)\ell^2.$$

Aus der Teilerfremdheit folgt $k^3 = \ell^2$, also ist $k = m^2$ und $\ell = m^3$ für ein $m \in \mathbf{N}$. ■

Höhenabschätzungen

Zunächst wollen wir abschätzen, wie sich die Höhe beim Addieren von rationalen Punkten verhält.

SATZ 62. *Sei E eine über $\mathbf{Q}$ definierte elliptische Kurve mit der Gleichung $y^2 = x^3 + ax + b$. Dann gibt es eine Konstante $c_1(E)$, so daß für alle $P_1, P_2 \in E(\mathbf{Q})$ gilt:*

$$H(P_1 + P_2) \leq c_1(E) \cdot H(P_1)^2 H(P_2)^2.$$

Man kann wählen

$$c_1(E) = 88H(E)^3.$$

Beweis: Dies folgt sofort, wenn wir unsere Additionstheoreme nehmen und ganz grob mit der Dreiecksungleichung abschätzen. ■

Wie gut ist diese Abschätzung? Setzt man $P_2 = -P_1$, so ist $H(P_1 + P_2) = H(O) = 1$.

FOLGERUNG 23.

$$H(2P) \leq c_1(E) \cdot H(P)^4.$$

Wir wollen nun zeigen, daß auch eine Ungleichung in der anderen Richtung gilt.

Satz 63. *Es gibt eine Konstante $c_2 = c_2(E)$, so daß gilt*

$$\frac{1}{c_2}H(P)^4 \leq H(2P).$$

Man kann wählen

$$c_2(E) = 237367H(E)^9.$$

Beweis:

- Wir schreiben $f = x_1^3 + ax_0^2x_1 + bx_0^3 - x_0x_2^2$ mit $a, b \in \mathbf{Z}$ und betrachten jetzt die Multiplikation mit 2. Die beiden ersten unserer Additionsformeln verschwinden identisch, die dritte wird

$$2 \cdot (x_0 : x_1 : x_2) = (f_0 : f_1 : f_2)$$

mit

$$\begin{array}{rcl} f_0 & = & 2x_2(3bx_0^3 + 3ax_0^2x_1 + x_2^2x_0 + 3x_1^3) : \\ f_1 & = & 2x_2(a^2x_0^3 - 9bx_0^2x_1 - 3ax_0x_1^2 + x_2^2x_1) : \\ f_2 & = & -x_0^4a^3 - 9x_0^4b^2 - 6abx_0^3x_1 - 6a^2x_1^2x_0^2 + 18bx_1^3x_0 + 3ax_1^4 + x_2^4 \end{array}$$

- Da $(f_0 : f_1 : f_2)$ einen Morphismus von $E \to \mathbf{P}^2$ liefert, ist

$$\{P \in \mathbf{P}^2 : f(P) = f_0(P) = f_1(P) = f_2(P) = 0\} = \emptyset.$$

Nach der projektiven Version des Hilbertschen Nullstellensatzes gilt dann im Polynomring $\mathbf{Q}[x_0, x_1, x_2]$:

$$\sqrt{(f_0, f_1, f_2, f)} = (x_0, x_1, x_2).$$

Daher gibt es einen Exponenten m mit

$$x_0^m, x_1^m, x_2^m \in (f_0, f_1, f_2, f).$$

D.h. es gibt Formen $\tilde{g}_{ij}$ vom Grad $m-3$ und $\tilde{g}_j$ vom Grad $m-2$ mit

$$\tilde{g}_{i0}f_0 + \tilde{g}_{i1}f_1 + \tilde{g}_{i2}f_2 + \tilde{g}_if = x_i^m$$

für $i = 0, 1, 2$.
- Wir probieren und finden für $m = 7$ Lösungen. Sie sind nicht eindeutig bestimmt. Im folgenden geben wir Beispiellösungen an:

- Definiert man

$$
\begin{aligned}
g_{00} &= x_2(-36x_0x_1ab - 56x_0^2a^3 + 60a^2x_1^2 + 405x_0^2b^2) \\
g_{01} &= 6x_2(-28x_0x_1a^2 + 69x_0^2ab + 9x_1^2b) \\
g_{02} &= -128x_0^3a^3 - 324x_0^3b^2 - 108x_1^3b + 108ax_0^2x_1b - 144a^2x_0x_1^2 \\
g_0 &= 252x_0^4ba^3 + 2916x_0^4b^3 - 360a^2x_1^2x_2^2 + 486x_0^2x_2^2b^2 - 240x_0^2x_2^2a^3 + 1296a^2x_1^2x_0^2b \\
&\quad -912a^4x_0^3x_1 + 324ax_1^4b - 3888ax_0^3x_1b^2 + 1944x_0x_1^3b^2 + 432x_0x_1^3a^3 \\
&\quad +864abx_0x_1x_2^2 \\
g_{10} &= -x_2(78x_0^2a^2b^3 - 4x_0x_1a^6 + 2a^4x_1^2b + 18x_0^2a^5b - 121x_0x_1b^2a^3 - 648x_0x_1b^4 \\
&\quad +36ax_1^2b^3) \\
g_{11} &= -x_2(-252ax_0x_1b^3 - 28a^4x_0x_1b + 51x_1^2a^2b^2 - 87x_0^2b^2a^3 - 432x_0^2b^4 + 8x_1^2a^5) \\
g_{12} &= 30b^3x_0^3a^2 - 216ab^3x_0x_1^2 - 40a^4bx_0x_1^2 + 16x_1^3a^5 - 26x_0^2x_1b^2a^3 + 102x_1^3a^2b^2 \\
&\quad -216x_0^2x_1b^4 \\
g_1 &= -126b^3a^2x_0^2x_2^2 - 36ba^5x_0^2x_2^2 - 1188b^3x_1^3x_0a^2 - 168bx_1^3x_0a^5 + 8x_0x_1x_2^2a^6 \\
&\quad +390x_0x_1x_2^2b^2a^3 + 1944x_0x_1x_2^2b^4 - 1296ax_0^2x_1^2b^4 - 12a^4x_0^2x_1^2b^2 \\
&\quad -540b^3x_0^3x_1a^3 - 56bx_0^3x_1a^6 + 16a^7x_0^2x_1^2 + 80x_1^4a^6 + 5832x_1^4b^4 + 270x_0^4a^2b^4 \\
&\quad -1944b^5x_0^3x_1 + 12a^4bx_1^2x_2^2 + 216ab^3x_1^2x_2^2 + 1422x_1^4b^2a^3 + 30x_0^4a^5b^2 \\
g_{20} &= x_0(36ax_0x_1b + 12a^2x_1^2 - 8a^3x_0^2 - 27x_0^2b^2)(4a^3 + 27b^2)^2 \\
g_{21} &= -6x_0(-3x_0^2ab - 4a^2x_0x_1 + 9x_1^2b)(4a^3 + 27b^2)^2 \\
g_{22} &= -4x_2(9bx_0^2 + 6x_0x_1a - 2x_2^2)(4a^3 + 27b^2)^2 \\
g_2 &= -6x_2(27b^2x_0^3 + 4x_0^3a^3 + 6x_2^2x_0b + 4x_1x_2^2a)(4a^3 + 27b^2)^2
\end{aligned}
$$

  so gilt für $i = 0, 1, 2$:

$$g_{i0}f_i + g_{i1}f_1 + g_{i2}f_2 + g_if_i = 8\Delta^2x_i^7.$$

  Durch ganz naives Abschätzen erhält man für $i = 0, 1, 2$:

$$|g_{i0}| + |g_{i1}| + |g_{i2}| \leq 237367H(C)^9H(P)^3.$$

- Seien jetzt $x_0, x_1, x_2 \in \mathbf{Z}$ paarweise teilerfremd mit $P = (x_0 : x_1 : x_2) \in E(\mathbf{Q})$. Wir setzen in die Formeln ein. Dann gilt $2 \cdot P = (f_0 : f_1 : f_2)$. Aus obigen Formeln sieht man dann, daß

$$ggT(f_0, f_1, f_2)|8\Delta^2$$

  gilt. D.h.

$$H(2P) = \frac{\max(|f_0|, |f_1|, |f_2|)}{ggT(f_0, f_1, f_2)} \geq \frac{\max(|f_0|, |f_1|, |f_2|)}{8\Delta^2}.$$

  Man beachte jetzt, daß $f(x_0, x_1, x_2) = 0$ gilt. Sei $|x_k| = H(P)$. Einsetzen liefert

$$H(P)^7 = |x_k|^7 \leq \frac{1}{8\Delta^2}(|g_{k0}| + |g_{k1}| + |g_{k2}|)\max(|f_0|, |f_1|, |f_2|) \leq 237367H(C)^3H(P)^3H(2P),$$

  woraus sofort

$$H(2P) \geq \frac{1}{237367H(C)^9}H(P)^4$$

  folgt. ■

Beispiel: Wir betrachten wieder unsere Kurve $y^2 = x^3 - 25x$. Schätzt man nach dem gleichen Verfahren ab, so erhält man

$$H(P_1 + P_2) \leq 19451H(P_1)^2H(P_2)^2$$

und

$$H(2P) \geq \frac{1}{2^4 \cdot 5^8 \cdot 61 \cdot 607}H(P)^4 \approx 0.43 \cdot 10^{-11}H(P)^4.$$

Wählt man jetzt $P = (1 : 45 : 300)$ und setzt $P_n = 2^nP$, so wird für $n = 0, 1, 2, \ldots$ die Folge $\frac{H(2P_n)}{H(P_n)^4}$:

$$0.7688765432 * 10^{-5}, 1.111119336, 199.7703833, 0.9999841825, 0.9997468485, 0.9959311040$$

Ohne Beweis geben wir noch folgendes Parallelogrammgesetz an:

SATZ 64. *Es gibt Konstanten $c_3(E), c_4(E) > 0$, so daß für alle Punkte $P_1, P_2 \in E(\mathbf{Q})$ gilt*

$$\frac{1}{c_4(E)} H(P_1)^4 H(P_2)^4 \leq H(P_1 + P_2) H(P_1 - P_2) \leq c_3(E) H(P_1)^4 H(P_2)^4.$$

Bemerkung: Der folgende Grenzwert exisitiert

$$h(P) = \lim_{n \to \infty} \frac{\ln H(2^n P)}{4^n}$$

und definiert eine quadratische Form, die sogenannte Neron-Tate-Höhe.

Torsionspunkte

Aus den Höhenabschätzungen erhält man sofort den

SATZ 65. *Die Gruppe $E(\mathbf{Q})_{tor}$ ist endlich. Für $P \in E(\mathbf{Q})_{tor}$ gilt:*

$$H(P) \leq c_2(E)^{1/3}.$$

Beweis: Sei $P \in E(\mathbf{Q})$ ein Torsionspunkt. Sei G die von P erzeugte Gruppe in $E(\mathbf{Q})$. Natürlich ist G endlich. Sei $P_m \in G$ ein Punkt maximaler Höhe in G. Dann gilt $H(2P_m) \leq H(P_m)$. Wenden wir jetzt unsere Abschätzung an, so erhalten wir

$$\frac{1}{c_2} H(P_m)^4 \leq H(2P_m) \leq H(P_m)$$

und damit

$$H(P) \leq H(P_m) \leq c_2(E)^{1/3}.$$

Da es nur endlich viele Punkte mit Höhe $\leq c_2^{1/3}$ gibt, folgt sofort die Behauptung. ∎

Man kann allerdings noch wesentlich mehr sagen. Wir zitieren hier nur als Beispiel einen Satz:

SATZ 66 (Lutz–Nagell). *Ist E eine elliptische Kurve mit der Gleichung $y^2 = x^3 + ax + b$, $a, b \in \mathbf{Z}$ und $P = (x, y) \in E(\mathbf{Q})_{tor}$, so gilt $x, y \in \mathbf{Z}$ und*

$$y = 0 \qquad \text{oder} \qquad y^2 | 4a^3 + 27b^2.$$

Beispiel: Wir betrachten wieder E mit $y^2 = x^3 - 25x$. Die 2-Teilungspunkte kennen wir schon. Wäre $P = (x, y) \in E(\mathbf{Q})_{tor}$, aber kein 2-Teilungspunkt, so würde $x, y \in \mathbf{Z}$ und $y^2 | 4(-25)^3 = (2 \cdot 5^3)^2$, also $y | 2 \cdot 5^3$ folgen. Durch Ausprobieren findet man, daß es keinen solchen Punkt gibt. Also

$$E(\mathbf{Q})_{tor} = \{O, (0,0), (5,0), (-5,0)\} \simeq \mathbf{Z}/2 \times \mathbf{Z}/2.$$

Descente — Abstieg

Unser Hauptziel ist der Beweis des folgendes Satzes:

SATZ 67 (Mordell–Weil). *Für eine über $\mathbf{Q}$ definierte elliptische Kurve ist die Gruppe $E(\mathbf{Q})$ der $\mathbf{Q}$-rationalen Punkte endlich erzeugt.*

Das bedeutet: alle rationalen Punkte auf E lassen sich durch Tangenten- und Sekantenbildung aus endlich vielen Punkten herleiten.

Ist A eine endlich erzeugte abelsche Gruppe, so ist natürlich auch $A/2A$ endlich erzeugt, also ein endlich dimensionaler $\mathbf{F}_2$-Vektorraum, also endlich. In unserem Fall gilt davon auch die Umkehrung:

LEMMA 16. *Sei $y^2 = x^3 + ax + b$ eine elliptische Kurve E über $\mathbf{Q}$ mit $a, b \in \mathbf{Z}$. Wir setzen voraus, daß $E(\mathbf{Q})/2E(\mathbf{Q})$ endlich ist. Seien dann $R_1, \ldots, R_m \in E(\mathbf{Q})$ Repräsentanten aller Klassen von $E(\mathbf{Q})/2E(\mathbf{Q})$. Setzt man $c_R = \max(H(R_1), \ldots, H(R_m))$, so enthält die Menge*

$$U = \{P \in E(\mathbf{Q}) : H(P) \leq \sqrt{c_1(E) c_2(E)} c_R\}$$

ein Erzeugendensystem von $E(\mathbf{Q})$. Insbesondere ist $E(\mathbf{Q})$ dann endlich erzeugt.

Beweis: Wir wollen sehen, daß alle Punkte $P \in E(\mathbf{Q})$ Linearkombination von Punkten aus U sind. Wir machen Induktion nach $H(P)$:
Gilt $H(P) \leq \sqrt{c_1 c_2} c_R$, so ist $P \in U$ und wir sind fertig.
Sei also $H(P) > \sqrt{c_1 c_2} c_R$. Es gibt einen Index i mit $P \equiv R_i \bmod 2E(\mathbf{Q})$. Also gibt es ein $Q \in E(\mathbf{Q})$ mit

$$P - R_i = 2Q.$$

Mit unseren Abschätzungen folgt

$$\frac{1}{c_2} H(Q)^4 \leq H(2Q) = H(P - R_i) \leq c_1 H(P)^2 H(R_i)^2 \leq c_1 c_R^2 H(P)^2$$

und damit

$$H(Q)^4 \leq c_1 c_2 c_R^2 H(P)^2 < H(P)^2 H(P)^2 = H(P)^4,$$

also $H(Q) < H(P)$. Nach Induktionsvoraussetzung ist Q Linearkombination von Punkten aus U und damit auch P wegen $P = R_i + 2Q$ und $R_i \in U$. ■

Schwacher Satz von Mordell-Weil

Wir müssen jetzt nur noch folgenden Satz zeigen:

SATZ 68 (Schwacher Mordell-Weil). *Ist E eine über $\mathbf{Q}$ definierte elliptische Kurve, so ist $E(\mathbf{Q})/2E(\mathbf{Q})$ endlich.*

Sei im folgenden E eine über $\mathbf{Q}$ definierte elliptische Kurve. Der Einfachkeit halber setzen wir voraus, daß alle 2-Torsionspunkte schon über $\mathbf{Q}$ definiert sind, d.h. E wird durch eine Gleichung

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \quad \text{mit } e_1, e_2, e_3 \in \mathbf{Z}$$

beschrieben. Ist dies nicht der Fall, muß man die Situation über einem Zahlkörper statt über $\mathbf{Q}$ studieren.

Vorbereitungen: Im folgenden rechnen wir viel mit der Gruppe $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$. Das Bild eines Elements $a \in \mathbf{Q}^\times$ in dieser Gruppe bezeichnen wir mit $\overline{a}$. Für $a, b \in \mathbf{Q}^\times$ gilt also

$$\overline{a} = \overline{b} \quad \Longleftrightarrow \quad b = ac^2 \text{ für ein } c \in \mathbf{Q}^\times.$$

Jedes Element dieser Gruppe hat eine eindeutige Darstellung

$$\overline{\pm p_1 p_2 \ldots p_r},$$

wo $p_1, \ldots, p_r$ verschiedene Primzahlen sind. Es gilt auch $\overline{a}^2 = \overline{1}$ und $\frac{1}{\overline{a}} = \overline{a}$. Sind keine Verwechslungen möglich, lassen wir das Überstreichen auch manchmal weg.
Weiter brauchen wir die Gruppe

$$N = \{(a_1, a_2, a_3) \in \mathbf{Q}^\times/\mathbf{Q}^{\times 2} \times \mathbf{Q}^\times/\mathbf{Q}^{\times 2} \times \mathbf{Q}^\times/\mathbf{Q}^{\times 2} : a_1 a_2 a_3 = 1\}.$$

Sei jetzt $P = (x, y) \in E(\mathbf{Q})$ mit $y \neq 0$. Dann gilt also

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

und daher in $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$:

$$\overline{(x - e_1)(x - e_2)(x - e_3)} = \overline{1}.$$

Also ist $(\overline{x - e_1}, \overline{x - e_2}, \overline{x - e_3}) \in N$ und folgende Definition ist sinnvoll:

DEFINITION 42. *Wir definieren $\phi : E(\mathbf{Q}) \to N$ durch*

$$\phi(P) = \left\{ \begin{array}{cc} (1,1,1) & \textit{falls } P = O \\ (x - e_1, x - e_2, x - e_3) & \textit{falls } P = (x,y), y \neq 0 \\ ((e_1 - e_2)(e_1 - e_3), e_1 - e_2, e_1 - e_3) & \textit{falls } P = (e_1, 0) \\ (e_2 - e_1, (e_2 - e_1)(e_2 - e_3), e_2 - e_3) & \textit{falls } P = (e_2, 0) \\ (e_3 - e_1, e_3 - e_2, (e_3 - e_1)(e_3 - e_2)) & \textit{falls } P = (e_3, 0) \end{array} \right\}$$

Im Prinzip kann man auf die dritte Komponente bei der Definition verzichten, da sie durch die ersten beiden bestimmt ist. Bevor wir die grundlegenden Eigenschaften von ϕ angeben, wollen wir ein Beispiel zeigen:

Beispiel: Sei E mit $y^2 = x^3 - 25x$. Wir wählen $e_1 = 0, e_2 = 5, e_3 = -5$ und erhalten dann $\phi : E(\mathbf{Q}) \to N$ mit

$$\phi((x,y)) = (\overline{x}, \overline{x-5}, \overline{x+5})$$

für $y \neq 0$ und entsprechend modifiziert für $y = 0$. Wir kennen bereits einige Punkte aus $E(\mathbf{Q})$ und berechnen dafür ϕ:

$$\begin{aligned}
\phi(O) &= (1,1,1), \\
\phi((0,0)) &= (-1,-5,5), \\
\phi((5,0)) &= (5,2,10), \\
\phi((-5,0)) &= (-5,-10,2), \\
\phi((-4,6)) &= (-1,-1,1), \\
\phi((\frac{25}{4}, \frac{75}{8})) &= (1,5,5), \\
\phi((-\frac{5}{9}, \frac{100}{27})) &= (-5,-2,10).
\end{aligned}$$

Es folgen einige Lemmatas:

Lemma 17. *ϕ ist ein Gruppenhomomorphismus.*

Beweis: Gilt $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, so rechnet man auf dem bekannten Weg aus, daß

$$x_3 = (\frac{y_1 - y_2}{x_1 - x_2})^2 - x_1 - x_2 + e_1 + e_2 + e_3$$

gilt. Dann findet man

$$(x_1 - e_1)(x_2 - e_1)(x_3 - e_1) = \frac{(x_1 y_2 - x_2 y_1 + e_1(y_1 - y_2))^2}{(x_1 - x_2)^2},$$

analog für e_2 und e_3, woraus der allgemeine Teil der Behauptung folgt. Die paar Ausnahmefälle kann man gesondert behandeln. ■

Lemma 18. *$Kern(\phi) = 2E(\mathbf{Q})$. Also erhalten wir*

$$E(\mathbf{Q})/2E(\mathbf{Q}) \hookrightarrow N.$$

Beweis: Ist $P \in E(\mathbf{Q})$, so ist $\phi(2P) = \phi(P)^2 = 1$, also folgt $2E(\mathbf{Q}) \subseteq kern(\phi)$. Explizit: Ist $P = (x,y)$ und $2P = (x_2, y_2)$, so erhält man

$$x_2 = \lambda^2 - 2x + e_1 + e_2 + e_3 \text{ mit } \lambda = \frac{3x^2 - 2(e_1 + e_2 + e_3)x + (e_1 e_2 + e_1 e_3 + e_2 e_3)}{2y}.$$

Damit wird

$$x_2 - e_1 = (\frac{x^2 - 2e_1 x + e_1 e_2 + e_1 e_3 - e_2 e_3}{4y})^2.$$

Also folgt $2E(\mathbf{Q}) \subseteq Kern(\phi)$. Zur Umkehrung: Sei $P = (x,y) \in Kern(\phi)$. Dann gibt es $a_i \in \mathbf{Q}$ mit $x - e_i = a_i^2$. Dann ist o.E. $y = a_1 a_2 a_3$. Indem man obige Gleichung nach x aufzulösen versucht, findet man 4 Lösungen. Es gilt z.B.

$$2(e_1 + a_1^2 + a_1 a_2 + a_1 a_3 + a_2 a_3, (a_1 + a_2)(a_1 + a_3)(a_2 + a_3)) = (x,y).$$

Damit folgt dann die Behauptung. ■

Wir wollen jetzt sehen, daß das Bild von ϕ endlich ist. Dazu definieren wir in Abhängigkeit von E

DEFINITION 43. *Für $b_1, b_2, b_3 \in \mathbf{Q}$ mit $(\overline{b_1}, \overline{b_2}, \overline{b_3}) \in N$ sei als Teilmenge des $\mathbf{P}^3$ definiert*

$$\begin{aligned} C_{(b_1,b_2,b_3)} &= \{e_1 z_0^2 + b_1 z_1^2 = e_2 z_0^2 + b_2 z_2^2 = e_3 z_0^2 + b_3 z_3^2 = 0\} = \\ &= \{(e_1 - e_2) z_0^2 + b_1 z_1^2 - b_2 z_2^2 = 0, \\ &\quad (e_2 - e_3) z_0^2 + b_2 z_2^2 - b_3 z_3^2 = 0, \\ &\quad (e_3 - e_1) z_0^2 + b_3 z_3^2 - b_1 z_1^2 = 0\}. \end{aligned}$$

LEMMA 19. *Für $(\overline{b_1}, \overline{b_2}, \overline{b_3}) \in N$ gilt:*

$$(\overline{b_1}, \overline{b_2}, \overline{b_3}) \in Bild(\phi) \quad \Longleftrightarrow \quad C_{b_1 b_2 b_3}(\mathbf{Q}) \neq \emptyset.$$

Beweis: $\Rightarrow$: Ist (b_1, b_2, b_3) das Bild von (x, y), so gibt es $q_i \in \mathbf{Q}$ mit $x - e_i = b_i q_i^2$. Es folgt

$$e_1 + b_1 q_1^2 = e_2 + b_2 q_2^2 = e_3 + b_3 q_3^2,$$

also ist

$$(1 : q_1 : q_2 : q_3) \in C_{(b_1,b_2,b_3)}(\mathbf{Q}).$$

$\Leftarrow$: Es gibt ein $q \in \mathbf{Q}^\times$ mit $b_1 b_2 b_3 = q^2$.
1. Fall: $(1 : q_1 : q_2 : q_3) \in C_{(b_1,b_2,b_3)}(\mathbf{Q})$. Dann ist

$$x = e_i + b_i q_i^2$$

unabhängig von i definiert und es gilt

$$(x - e_1)(x - e_2)(x - e_3) = b_1 q_1^2 b_2 q_2^2 b_3 q_3^2 = (q q_1 q_2 q_3)^2,$$

woraus sofort

$$P = (e_i + b_i q_i^2, q q_1 q_2 q_3) \in E(\mathbf{Q}) \quad \text{und } \phi(P) = (\overline{b_1}, \overline{b_2}, \overline{b_3})$$

folgt.
2. Fall: $(0 : q_1 : q_2 : q_3) \in C_{(b_1,b_2,b_3)}(\mathbf{Q})$. Dann ist

$$b_1 q_1^2 = b_2 q_2^2 = b_3 q_3^2,$$

also $\overline{b_1} = \overline{b_2} = \overline{b_3}$, woraus wegen $\overline{b_1 b_2 b_3} = \overline{1}$ sofort $\overline{b_1} = \overline{b_2} = \overline{b_3} = \overline{1}$ folgt. Dies ist aber das Urbild von O.
■

Unser Ziel ist es jetzt zu sehen, daß $C_{(b_1,b_2,b_3)}(\mathbf{Q})$ fast immer leer ist.

LEMMA 20. *Definiert man*

$$\begin{aligned} N_0 = \{(\overline{b_1}, \overline{b_2}, \overline{b_3}) \in N : \quad & b_1, b_2, b_3 \in \mathbf{Z} \textit{ quadratfrei, } b_1 b_2 b_3 \textit{ Quadrat,} \\ & p | b_1, p | b_2 \Rightarrow p | e_1 - e_2, \\ & p | b_1, p | b_3 \Rightarrow p | e_1 - e_3, \\ & p | b_2, p | b_3 \Rightarrow p | e_2 - e_3\}, \end{aligned}$$

so gilt für $(\overline{b_1}, \overline{b_2 b_3}) \in N$:

$$C_{(b_1,b_2,b_3)} \neq \emptyset \quad \Rightarrow (\overline{b_1}, \overline{b_2}, \overline{b_3}) \in N_0.$$

Damit folgt

$$Bild(\phi) \subseteq N_0.$$

Beweis: Sei $b_1, b_2, b_3 \in \mathbf{Z}$ quadratfrei und $(z_0 : z_1 : z_2 : z_3) \in C_{b_1 b_2 b_3}(\mathbf{Q})$, $z_0, z_1, z_2, z_3 \in \mathbf{Z}$ und $ggT(z_0, z_1, z_2, z_3) = 1$. Dann ist $b_1 b_2 b_3$ Quadrat in $\mathbf{Z}$.

- Gilt $p | b_1$, so folgt entweder $p | b_2$ oder $p | b_3$.
- Wir betrachten den Fall $p | b_1, p | b_2$ und $p \not| b_3$. Modulo p folgt

  $$e_1 z_0^2 \equiv e_2 z_0^2 \equiv e_3 z_0^2 + b_3 z_3^2 \bmod p,$$

  also auch $z_0^2 (e_1 - e_2) \equiv 0 \bmod p$.
  Fall: $z_0 \equiv 0 \bmod p$. Dann folgt $z_3 \equiv 0 \bmod p$. Wir betrachten jetzt die Gleichung

  $$e_1 z_0^2 + b_1 z_1^2 = e_2 z_0^2 + b_2 z_2^2 = e_3 z_0^2 + b_3 z_3^2$$

  modulo p^2 und erhalten

  $$b_1 z_1^2 \equiv b_2 z_2^2 \equiv 0 \bmod p^2,$$

was $z_1 \equiv z_2 \equiv 0 \bmod p$ liefert, einen Widerspruch zu $ggT(z_0, z_1, z_2, z_3) = 1$.
Also kann dieser Fall nicht eintreten und es bleibt nur noch $p|e_1 - e_2$ übrig.

- Analog gehen die anderen Fälle. Also gilt:

$$\begin{aligned} p|b_1, b_2 &\Rightarrow p|e_1 - e_2, \\ p|b_1, b_3 &\Rightarrow p|e_1 - e_3, \\ p|b_2, b_3 &\Rightarrow p|e_2 - e_3, \end{aligned}$$

was wir zeigen wollten. ■

Nun ist aber N_0 endlich, womit schließlich der schwache Satz von Mordell-Weil bewiesen ist.

FOLGERUNG 24 (Schwacher Satz von Mordell-Weil). *Für eine elliptische Kurve E über $\mathbf{Q}$ ist $E(\mathbf{Q})/2E(\mathbf{Q})$ endlich.*

Hiermit ist dann auch der Satz von Mordell-Weil (zumindest unter unseren Voraussetzungen) bewiesen, den wir nochmals angeben unter Verwendung des Hauptsatzes über endlich erzeugte abelsche Gruppen:

SATZ 69 (Mordell-Weil). *Ist E eine über $\mathbf{Q}$ definierte elliptische Kurve, so ist $E(\mathbf{Q})$ endlich erzeugt, d.h.*

$$E(\mathbf{Q}) \simeq E(\mathbf{Q})_{tor} \oplus \mathbf{Z}^r.$$

Dabei ist $E(\mathbf{Q})_{tor}$ endlich. r heißt der Rang der elliptischen Kurve.

Beispiel: Wir betrachten wieder $y^2 = x^3 - 25x$.

1. Bei Wahl von $e_1 = 0, e_2 = 5, e_3 = -5$ ist die Abbildung $\phi : E(\mathbf{Q}) \to \mathbf{Q}^\times/\mathbf{Q}^{\times 2} \times \mathbf{Q}^\times/\mathbf{Q}^{\times 2} \times \mathbf{Q}^\times/\mathbf{Q}^{\times 2}$ durch
$$\phi((x,y) = (\overline{x}, \overline{x-5}, \overline{x+5})$$
gegeben. Man beachte, daß $Bild(\phi)$ eine Untergruppe ist.
2. Wir hatten bereits gesehen:
$$\{(1,1,1), (-1,-5,5), (5,2,10), (-5,-10,2), (-1,-1,1), (1,5,5), (-5,-2,10)\} \subseteq Bild(\phi).$$
Als Untergruppe gilt dann auch noch $(5,10,2) \in Bild(\phi)$, also
$$8|\#Bild(\phi).$$
3. Was kann man über die Vorzeichen der b_i's mit $(\overline{b_1}, \overline{b_2}, \overline{b_3}) \in Bild(\phi)$ sagen? Wegen $\phi((x,y)) = (x, x-5, x+5)$ gibt es nur zwei Möglichkeiten:
$$(+,+,+) \quad \text{oder} \quad (-,-,+).$$
4. Nun ist $e_1 - e_2 = -5$, $e_1 - e_3 = 5$, $e_2 - e_3 = 10$, woraus sich für N_0 ergibt:
$$\begin{aligned} N_0 \quad = \quad & \{(\overline{b_1}, \overline{b_2}, \overline{b_3}) \in N : (|b_1|, |b_2|, |b_3|) = \\ & (1,1,1), (1,2,2), (1,5,5), (1,10,10), (5,1,5), (5,2,10), (5,5,1), (5,10,2)\}. \end{aligned}$$
5. Unter Beachtung der möglichen Vorzeichen erhält man damit, daß das Bild von ϕ in folgender Gruppe liegt:
$$\begin{aligned} N_1 \quad = \quad & \{(\pm 1, \pm 1, 1), (\pm 1, \pm 2, 2), (\pm 1, \pm 5, 5), (\pm 1, \pm 10, 10), \\ & (\pm 5, \pm 1, 5), (\pm 5, \pm 2, 10), (\pm 5, \pm 5, 1), (\pm 5, \pm 10, 2)\}. \end{aligned}$$
6. Da $Bild(\phi)$ eine Gruppe ist, bleiben nur zwei Möglichkeiten: $\#Bild(\phi) \in \{8, 16\}$. Wir betrachten zum Beispiel
$$C_{(1,2,2)} = \{5z_0^2 - z_1^2 + 2z_2^2 = 0 \text{ und } 5z_0^2 + z_1^2 - 2z_3^2 = 0\}.$$
Wir nehmen an: $(z_0 : z_1 : z_2 : z_3) \in C_{(1,2,2)}(\mathbf{Q})$ mit $z_i \in \mathbf{Z}$ und $ggT(z_0, z_1, z_2, z_3) = 1$. Nun folgt modulo 5 sofort $z_1^2 \equiv 2z_2^2$, also $z_1 \equiv z_2 \equiv 0 \bmod 5$ und damit nacheinander $z_0 \equiv 0 \bmod 5$ und $z_3 \equiv 0 \bmod 5$, was schlie3lich einen Widerspruch liefert. Also ist $C_{(1,2,2)}(\mathbf{Q}) = \emptyset$ und damit $(1,2,2) \notin Bild(\phi)$.
7. $Bild(\phi)$ hat also 8 Elemente, nämlich:
$$(1,1,1), (-1,-5,5), (5,2,10), (-5,-10,2), (-1,-1,1), (1,5,5), (-5,-2,10), (5,10,2).$$

8. Wegen
$$E(\mathbf{Q}) \simeq E(\mathbf{Q})_{tor} \oplus \mathbf{Z}^r = \mathbf{Z}/2 \oplus \mathbf{Z}/2 \oplus \mathbf{Z}^r$$
ist also nun
$$(\mathbf{Z}/2)^3 \simeq E(\mathbf{Q})/2E(\mathbf{Q}) \simeq (\mathbf{Z}/2)^2 \oplus (\mathbf{Z}/2)^r,$$
also der Rang $r = 1$.
9. Wie erhält man daraus ein Erzeugendensystem für $E(\mathbf{Q})$? Wählt man
$$R_1 = O, R_2 = (1:0:0), R_3 = (1:5:0), R_4 = (1:-5:0), R_5 = (1:-4:6),$$
$$R_6 = R_2 + R_5 = (8:50:75), R_7 = R_3 + R_5 = (27:-15:-100), R_8 = R_4 + R_5 = (1:45:-300),$$
so sind die R_i's Repräsentanten von $E(\mathbf{Q})/2E(\mathbf{Q})$.
10. Es gilt nun
$$c_1 = 19451, \quad c_2 = 2^4 \cdot 5^8 \cdot 61 \cdot 607, \quad c_R = 300,$$
sodaß gilt
$$\sqrt{c_1 c_2} c_R \leq 2.0128 \cdot 10^{10},$$
also enthält
$$U = \{P \in E(\mathbf{Q}) : H(P) \leq 2.0128 \cdot 10^{10}\}$$
ein Erzeugendensystem von $E(\mathbf{Q})$. Das ist aber zum Ausprobieren zu groß. $\boxed{???}$
11. Es wird wohl gelten:
$$E(\mathbf{Q}) = \mathbf{Z}(0,0) + \mathbf{Z}(5,0) + \mathbf{Z}(-4,6).$$

Bemerkungen:

1. Der Satz von Mordell-Weil besagt für eine über $\mathbf{Q}$ definierte elliptische Kurve E, daß $E(\mathbf{Q})$ eine endlich erzeugte abelsche Gruppe ist. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen erhält man also eine Zerlegung
$$E(\mathbf{Q}) \simeq E(\mathbf{Q})_{tor} \oplus \mathbf{Z}^r.$$
r heißt der Rang der elliptischen Kurve E.
2. Längere Zeit vermutet, von Mazur 1977 bewiesen wurde folgende Aussage, deren Beweis die Vorlesung weit übersteigen würde: $E(\mathbf{Q})_{tor}$ ist eine der folgenden Gruppen:
$$\mathbf{Z}/n \quad \text{für } 1 \leq n \leq 10 \text{ oder } n = 12,$$
$$\mathbf{Z}/2 \times \mathbf{Z}/2n \quad \text{für } 1 \leq n \leq 4.$$
3. Wie groß der Rang r werden kann, ist nicht bekannt. Die Kurve
$$y^2 = x^3 - 101596938352x + 12361366202306320$$
hat Rang ≥ 12. Die Kurve
$$y^2 + 357573631y = x^3 + 2597055x^2 - 549082x - 19608054$$
hat Rang ≥ 14.
4. Ist der Rang groß, so hat E also viele rationale Punkte, sollte also auch viele Punkte modulo p haben. Dies haben Birch und Swinnerton-Dyer untersucht. Eine ihrer Vermutungen läßt sich so formulieren:
Sei $f(P) = \Pi_{p \leq P} \frac{\#E(\mathbf{F}_p)}{p}$. Dann gibt es Konstanten C_1 und C_2 mit
$$C_1(\ln P)^r \leq f(P) \leq C_2(\ln P)^r.$$
Dabei ist r der Rang. Bei der Betrachtung elliptischer Kurven über endlichen Körpern treten gewissen Faktoren auf:
$$\ell_p(s) = \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \quad \text{mit } a_p = p + 1 - \#E(\mathbf{F}_p).$$
Es gilt
$$\ell_p(1) = \frac{1}{1 - \frac{a_p}{p} + \frac{1}{p}} = (\frac{\#E(\mathbf{F}_p)}{p})^{-1}.$$

Definiert man

$$L_E(s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}},$$

so sollte gelten $L_E(1) = 0$ falls $r > 0$ und $L_E(1) \neq 0$, falls $r = 0$. Durch die Formel für $L_E(s)$ ist die Funktion noch nicht sinnvoll definiert. Als Dirichletreihe ist sie definiert für $Re(s) \geq \frac{3}{2}$. Es wird vermutet, daß L_E sich analytisch auf ganz $\mathbf{C}$ fortsetzen läßt und daß L_E eine Nullstelle der Ordnung r für $s = 1$ hat. Diese Vermutungen gehen auf Birch und Swinnerton-Dyer zurück und sind bis jetzt noch nicht allgemein bewiesen.

5. Es gibt keinen allgemeinen Algorithmus um $E(\mathbf{Q})$ bzw. den Rang oder ein Erzeugendensystem zu bestimmen. Das liegt hauptsächlich daran, daß man nicht allgemein testen kann, ob

$$C_{(b_1,b_2,b_3)}(\mathbf{Q})$$

leer ist oder nicht.

6. Für die Arithmetik elliptischer Kurven über $\mathbf{Q}$ gibt es APECS.

ANHANG A

Additionstheoreme für elliptische Kurven

In H. Lange, W. Ruppert, Addition Laws on Elliptic Curves in Arbitrary Characteristics, J. Algebra **107**, 106-116 sind für allgemeine elliptische Kurven

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Additionstheoreme angegeben in der Form

$$(x_0 : x_1 : x_2) + (y_0 : y_1 : y_2) = (z_{i0} : z_{i1} : z_{i2}).$$

Dabei ist allerdings ein Fehler in der Formel z_{31} passiert. Die richtigen Formeln ergeben sich aus:

```
b2:=a1^2+a2;
b3:=a1*a2-3*a3;
b4:=a1*a3+a4;
b5:=a1*a4-a2*a3;
b6:=a3^2+3*a6;
b7:=3*a1*a6-a3*a4;
b8:=a2*b6-a4*b4+a6*b2;
b9:=a1*b8-a3*b6;
b10:=(a2+b2)*b8-a3^2*b4-2*a4*b6;
b12:=b4*b8-b6^2;

S0:=x0^2; S2:=x0*x1; S3:=x0*x2; S4:=x1^2; S5:=x1*x2; S6:=x2^2;
T0:=y0^2; T2:=y0*y1; T3:=y0*y2; T4:=y1^2; T5:=y1*y2; T6:=y2^2;
for i from 0 to 6 do
for j from 0 to 6 do
P.i.j:=S.i*T.j;
Q.i.j:=P.i.j-P.j.i;
R.i.j:=P.i.j+P.j.i;
od;od;

# Z(1)
z10:=a4*Q02-a3*Q03+a2*Q04-a1*Q05-Q06+3*Q24;
z11:=-3*a6*Q02-a4*Q04+a3*Q05-2*a3*Q23-a2*Q24-Q26+a1*Q34+2*Q35;
z12:=b7*Q02+b6*Q03+b5*Q04+a4*Q05+2*b4*Q23+b3*Q24+2*a2*Q25-b2*Q34
-2*a1*Q35-Q36+3*Q45;

# Z(2)
z20:=b6*Q02+b4*Q04+a3*Q05+b2*Q24+2*a1*Q25+Q26+a1*Q34+2*Q35;
z21:=-b8*Q02-b6*Q04-b4*Q24-a3*Q34+a1*Q45+Q46;
z22:=b9*Q02+b8*Q03+b7*Q04+3*a6*Q05+2*b6*Q23+b5*Q24+2*a4*Q25-b4*Q34
-2*a3*Q35+a2*Q45+Q56;

# Z(3)
z30:=a3*b6*R00+3*(a1*a3^2+a1*a6+a3*a4)*R02+3*(a3^2+2*a6)*R03
+(a1*b4+a2*a3)*(R04+2*R22)+2*b4*(R05+2*R23)+a3*(R06+2*R33)
+(a1^3+3*a1*a2+3*a3)*R24+(a1^2+2*a2)*(2*R25+R34)+a1*(R26+2*R35)
```

```
+3*a1*R44+2*R36+6*R45;
z31:=-a3*b8*R00-(b9+3*a3*(a6+b6))*R02-2*b8*R03-(3*a1*a6+a3*b4)*(R04+2*R22)
-(a3^2+6*a6)*(R05+2*R23)-(3*a1*a4+a3*b2)*R24-2*a4*(2*R25+R34)
+a3*(R26+2*R35)-a1*a2*R44+(a1^2-2*a2)*R45+a1*R46+2*a1*R55+2*R56;
z32:=b12*R00+b10*R02+b9*R03+(2*b8+a6*b2-a2*b6)*(R04+2*R22)
+b7*(R05+2*R23)+(a1^2*a4-2*a2*b4+3*b6+9*a6)*R24+b5*(2*R25+R34)
-(a2^2-3*a4)*R44+a3*R36+(a1*a2-3*a3)*R45+a1*R56+R66;
```

Erläuterung: Wir beginnen mit

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Dies läßt sich auch schreiben

$$(y + \frac{1}{2}a_1x + \frac{1}{2}a_3)^2 = x^3 + (a_2 + \frac{1}{4}a_1^2)x^2 + (a_4 + \frac{1}{2}a_1a_3)x + (a_6 + \frac{1}{4}a_3^2).$$

Wir setzen jetzt

$$A = a_2 + \frac{1}{4}a_1^2, \quad B = a_4 + \frac{1}{2}a_1a_3, \quad C = a_6 + \frac{1}{4}a_3^2.$$

Wir benutzen die Transformationsformeln

$$X_0 = x_0, \quad X_1 = x_1, \quad X_2 = \frac{1}{2}a_3x_0 + \frac{1}{2}a_1x_1 + x_2$$

$$Y_0 = y_0, \quad Y_1 = y_1, \quad Y_2 = \frac{1}{2}a_3y_0 + \frac{1}{2}a_1y_1 + y_2$$

Dann berechnen wir die Additionsformeln Z_{i0}, Z_{i1}, Z_{i2} für $i = 1, 2, 3$ und transformieren mit

$$\tilde{z}_{i0} = Z_{i0}, \quad \tilde{z}_{i1} = Z_{i1}, \quad \tilde{z}_{i2} = -\frac{1}{2}a_3Z_{i0} - \frac{1}{2}a_1Z_{i1} + Z_{i2}$$

wieder zurück.

Fast immer gilt $\tilde{z}_{ij} = z_{ij}$, wo z_{ij} die in der Arbeit angebene Formel ist. Nur für $i = 3, j = 1$ ist ein Fehler passiert. Hier ist

$$\tilde{z}_{31} = z_{31} + a_1a_3^2(x_0^2y_1^2 + x_1^2y_0^2 + 4x_0x_1y_0y_1)$$

$$\begin{aligned} a_1a_3^2(x_0^2y_1^2 + x_1^2y_0^2 + 4x_0x_1y_0y_1) &= a_1a_3^2(S_0T_4 + S_4T_0 + 4S_2T_2) = \\ &= a_1a_3^2(P_{04} + P_{40} + 4P_{22}) = \\ &= a_1a_3^2(R_{04} + 2R_{22}) \end{aligned}$$

Angegeben ist

$$z_{31} = \cdots - (a_1b_6 + a_3b_4)(R_{04} + 2R_{22}) + \ldots,$$

richtig ist aber

$$\tilde{z}_{31} = \cdots - (3a_1a_6 + a_3b_4)(R_{04} + 2R_{22}) + \ldots$$

ANHANG B

Der Algorithmus von Vélu

SATZ 70. *Sei E eine elliptische Kurve mit der Gleichung $y^2 = x^3 + ax + b$ und $U \subseteq E$ eine Untergruppe mit n Elementen. Definiert man für $i = 1, 2, 3$*

$$p_i = \sum_{(u,v) \in U \setminus \{(0:0:1)\}} u^i$$

und

$$A = -(5n-6)a - 15p_2 \qquad \text{und} \qquad B = -(14n-15)b - 21ap_1 - 35p_3,$$

so hat E/U die Gleichung $y^2 = x^3 + Ax + B$.

Beispiel: Wir betrachten E mit der Gleichung $y^2 = x^3 + x + 2$ über $\mathbf{Q}$. Man rechnet nach, daß

$$U = \{O, (1,2), (1,-2), (-1,0)\}$$

eine Untergruppe ist. Hier ist also $n = 4, a = 1, b = 2, p_1 = 1, p_2 = 3, p_3 = 1$, woraus sich sofort $A = -14 - 45 = -59$ und $B = -82 - 21 - 35 = -138$ ergibt, d.h. $y^2 = x^3 - 59x - 138$ ist eine Gleichung für E/U.

ANHANG C

Bemerkungen zu Torsionspunkten elliptischer Kurven über Q

1. $y^2 = x^3 - 24300$ – Torsion über Q und über $\mathbf{F}_p$

Wir betrachten die über $\mathbf{Q}$ definierte elliptische Kurve

$$E : y^2 = x^3 - 2^2 \cdot 3^5 \cdot 5^2 = x^3 - 24300.$$

Die Kurve E ist nichtsingulär modulo p für $p \geq 7$, also gilt

$$E(\mathbf{Q})_{Torsion} \hookrightarrow E(\mathbf{F}_p).$$

Durch Abzählen findet man schnell $\#E(\mathbf{F}_7) = 3$, also hat man

$$E(\mathbf{Q})_{Torsion} \simeq 0 \text{ oder } \mathbf{Z}/3\mathbf{Z}.$$

(Durch weiteres Probieren findet man für alle p mit $7 \leq p \leq 47$ die Aussage $\#E(\mathbf{F}_p) \equiv 0 \bmod 3$? Gilt dies für alle $p \geq 7$ Warum?) Ist also $E(\mathbf{Q})_{Torsion}$ nichttrivial, so kann es nur 3-Teilungspunkte geben. Ist nun $(x, y) \in E(\mathbf{Q})$, so gilt

$$3 \cdot (x, y) = (\frac{x^9 + 2332800x^6 + 28343520000x^3 - 918330048000000}{9x^2(x^3 - 97200)^2}, \dots).$$

Wäre (x, y) ein 3-Teilungspunkt, so müßte x Nullstelle von $9x^2(x^3 - 97200)^2 = 9x^2(x^3 - 2^4 \cdot 3^5 \cdot 5^2)^2$ sein, also $x = 0$; es gibt aber keinen rationalen Punkt mit $x = 0$. Daher ist $3 \cdot (x, y) \neq 0$ und damit

$$E(\mathbf{Q})_{Torsion} = 0.$$

Wir wollen jetzt die 3-Torsion in $E(\mathbf{F}_p)$ untersuchen. Sei $p \geq 7$ eine Primzahl; die Kurve E ist dann nichtsingulär über $\mathbf{F}_p$. Ein nichttrivialer 3-Teilungspunkt existiert in $E(\mathbf{F}_p)$ genau dann, wenn es $x, y \in \mathbf{F}_p$ gibt mit

$$y^2 = x^3 - 2^2 \cdot 3^5 \cdot 5^2 \text{ und } x(x^3 - 2^4 \cdot 3^5 \cdot 5^2) = 0.$$

1. Fall: $p \equiv 1 \bmod 3$*:* Mit dem Gaußschen quadratischen Reziprozitätsgesetz folgt für das Legendre-Symbol

$$(\frac{-3}{p}) = (\frac{p}{3}) = 1,$$

d.h. -3 ist Quadrat modulo p, also gibt es $a \in \mathbf{F}_p$ mit $a^2 = -3$. Dann ist $(0, 2 \cdot 3^2 \cdot a \cdot 5)$ ein nichttrivialer 3-Teilungspunkt in $E(\mathbf{F}_p)$.

2. Fall: $p \equiv -1 \bmod 3$*:* Dann teilt 3 nicht $p - 1 = \#\mathbf{F}_p^\times$, also ist $x \mapsto x^3$ ein injektiver und damit auch surjektiver Gruppenautomorphismus von $\mathbf{F}_p^\times$. Deswegen gibt es ein $b \in \mathbf{F}_p$ mit $b^3 = 2^4 \cdot 3^5 \cdot 5^3$. Nun ist

$$b^3 - 2^4 \cdot 3^5 \cdot 5^2 = 2^4 \cdot 3^5 \cdot 5^3 - 2^4 \cdot 3^5 \cdot 5^2 = 2^2 \cdot 3^6 \cdot 5^2 = (2 \cdot 3^3 \cdot 5)^2,$$

also ist $(b, 2 \cdot 3^3 \cdot 5)$ ein nichttrivialer 3-Teilungspunkt in $E(\mathbf{F}_p)$.

Damit erhalten wir also für alle Primzahlen $p \geq 7$:

$$3 | \#E(\mathbf{F}_p).$$

Die Kurve E liefert also ein Beispiel einer Kurve mit

$$\#E(\mathbf{Q})_{Torsion} < ggT(\#E(\mathbf{F}_p) : E \text{ ist nichtsingulär modulo } p).$$

2. Torsionpunkte auf $y^2 = x^3 + ax^2 + bx + c$

SATZ 71. *Ist $y^2 = x^3 + ax^2 + bx + c$ eine elliptische Kurve über $\mathbf{Q}$ mit $a, b, c \in \mathbf{Z}$ und $P = (x, y)$ ein über $\mathbf{Q}$ definierter Torsionspunkt mit $y \neq 0$, so gilt*

$$y^2 | D, \qquad \textit{wo} \qquad D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

die Diskriminante (des kubischen Polynoms) ist.

Beweis: Ist $P = (x, y)$ und $2P = (x_2, y_2) \neq O$, so gilt

$$x_2 = \frac{Z}{4N}$$

mit

$$\begin{aligned} Z &= x^4 - 2bx^2 - 8cx - 4ac + b^2 \\ N &= x^3 + ax^2 + bx + c = y^2 \end{aligned}$$

Setzt man jetzt $g = u_3x^3 + u_2x^2 + u_1x + u_0$ und $h = v_2x^2 + v_1x + v_0$ mit unbestimmten Koeffizienten an und versucht die Koeffizienten so zu bestimmen, daß $Ng + Zh$ konstant ist, so findet man

$$\begin{aligned} g &= 3x^3 - ax^2 - 5bx + 2ab - 27c \\ h &= 3x^2 - 2ax + a^2 - 4b \end{aligned}$$

und die Beziehung

$$Ng + Zh = D.$$

Division durch $N = y^2$ liefert

$$\frac{D}{y^2} = g + 4hx_2.$$

Ist nun P ein Torsionspunkt, so auch $2P$. Wir wissen bereits, daß dann x, y, x_2, y_2 ganze Zahlen sind, also gilt auch $x, x_2, g(x), h(x) \in \mathbf{Z}$. Damit folgt $\frac{D}{y^2} \in \mathbf{Z}$, also

$$y^2 | D,$$

was wir zeigen wollten. ■

ANHANG D

Vorlesungsankündigung

MATHEMATISCHES INSTITUT
UNIVERSITÄT ERLANGEN-NÜRNBERG
Priv.-Doz. Dr. W. Ruppert

Bismarckstraße $1\frac{1}{2}$, 12. Juli 1995
D-91054 Erlangen
Telefon: 09131/852466

Vorlesungsankündigung
für das Wintersemester 1995/96

Diophantische Geometrie

Rationale Punkte auf algebraischen Kurven

Ein Grundproblem der Zahlentheorie ist das Lösen diophantischer Gleichungen; behandelt man diese Fragestellung mit geometrischen Methoden, so betreibt man Diophantische Geometrie. In der Vorlesung soll es um rationale Lösungen von Gleichungen der Form $f(x,y) = 0$ gehen, wo f ein Polynom mit rationalen Koeffizienten ist. Betrachtet man $f(x,y) = 0$ geometrisch, so erhält man eine algebraische Kurve C. Unsere Ausgangsfrage übersetzt sich dann in die Frage nach den rationalen Punkten auf der Kurve C. Einer algebraischen Kurve läßt sich nun (auf verschiedene Weisen) eine ganze Zahl $g \geq 0$, das sogenannte Geschlecht von C zuordnen. (Ist $f(x,y)$ vom Grad d und $f(x,y) = 0$ ohne Singularitäten, so ist $g = \frac{(d-1)(d-2)}{2}$.) In Abhängigkeit vom Geschlecht g einer Kurve C hat man folgende Aussagen über rationale Punkte auf C:
Hat eine Kurve C vom Geschlecht 0 einen rationalen Punkt, so gleich unendlich viele, die sich durch rationale Funktionen $x = \alpha(t)$ und $y = \beta(t)$ parametrisieren lassen. Z.B. erhält man alle rationalen Lösungen von $x^2 + y^2 = 5$ durch die Parametrisierung $x = \frac{t^2-4t-1}{t^2+1}$ und $y = \frac{2t^2+2t-2}{t^2+1}$.
Hat eine Kurve C vom Geschlecht 1 einen rationalen Punkt, so läßt sich geometrisch eine Verknüpfung definieren, wodurch die Menge der rationalen Punkte auf C eine abelsche Gruppe wird. (Man spricht von einer elliptischen Kurve.) Mordell hat 1922 gezeigt, daß diese Gruppe endlich erzeugt ist. Z.B. bilden die rationalen Punkte auf $x^3 + y^3 = 19$ eine zu $\mathbf{Z} \times \mathbf{Z}$ isomorphe Gruppe, die Verknüpfung entsteht durch Sekanten- und Tangentenbildung.
Mordell hat 1922 vermutet, daß jede Kurve vom Geschlecht $g \geq 2$ nur endlich viele rationale Punkte besitzt. Den ersten Beweis dafür gab Faltings 1983; ein elementarer Beweis stammt von Bombieri aus dem Jahr 1990, der in der Vorlesung behandelt werden soll.

Die 4-stündige Vorlesung will in den Problemkreis der Diophantischen Geometrie an Hand der Frage nach rationalen Punkten auf algebraischen Kurven einführen. Es ist eine Spezialvorlesung aus dem Bereich Zahlentheorie/Algebraische Geometrie. Hörer sollten Kenntnisse der Algebra und Funktionentheorie besitzen. Im Vorgehen wird sich die Vorlesung den Vorkenntnissen der Hörer anpassen und gegebenenfalls benötigte weitere Hilfsmittel bereitstellen.

Zeit und Ort: Di, Do 8-10, Übungsraum 3
Beginn: 2. November 1995
Nummer im Vorlesungsverzeichnis:

gez. W. Ruppert

Literaturverzeichnis

[Cornell/Silverman] G. Cornell, J. H. Silverman (editors), Arithmetic Geometry, Springer 1986.
[Hartshorne] R. Hartshorne, Algebraic Geometry, Springer 1977.
[Lang1] S. Lang, Fundamentals of Diophantine Geometry, Springer 1983.
[Lang2] S. Lang, Number Theory III - Diophantine Geometry, Springer1991.
[Mordell] L. J. Mordell, Diophantine Equations, Academic Press 1969.
[Serre] J.-P. Serre, Lectures on the Mordell-Weil Theorem, Vieweg 1989.
[Silverman] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer 1986.