KAPITEL 11

Kurven vom Geschlecht 0

1. Allgemeines zu Kurven vom Geschlecht 0

Wenn nichts anderes erwähnt wird, bezeichnet C eine absolut irreduzible, nichtsinguläre, projektive Kurve, die über einem vollkommenen Körper K definiert ist. (Für $g = 0$ lautet Riemann-Roch $\ell(D) = \operatorname{grad}(D) + 1$ für $\operatorname{grad}(D) \geq -1$.)

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

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

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

Beweis:

- *1. Beweis:* Aus $\operatorname{grad}(D) = 1$ folgt $\ell(D) = 2$. Sei f_0, f_1 eine K-Basis von $\mathcal{L}(D)$. Wegen $\operatorname{grad}(D) = 1 = 2{\cdot}0{+}1$ ist D sehr ampel, also $\phi : C \to \mathbb{P}^1$ mit $\phi = (f_0 : f_1)$ eine Einbettung, d.h. $C \simeq \phi_D(C)$. Nun ist aber $\phi_D(C) = \mathbb{P}^1$, also ϕ_D ein Isomorphismus.
- *2. Beweis:* Aus $\operatorname{grad}(D) = 1$ folgt $\ell(D) = 2$, also gibt es ein $f \in K(C) \cap \mathcal{L}(D)$ mit $D + \operatorname{div}(f) \geq 0$, also einen Punkt $P \in C(K)$ mit $D + \operatorname{div}(f) = [P]$. Es ist $\ell([P]) = 2$, also gibt es eine Funktion $g \in K(C) \cap \mathcal{L}([P])$ mit $\mathcal{L}([P]) = \overline{K} + \overline{K}g$. Dann hat g genau eine Polstelle, und zwar in P mit $\operatorname{ord}_P(g) = -1$. Deshalb hat der zugehörige Morphismus $\phi = (1 : g) : C \to \mathbb{P}^1$ Grad 1, was $K(\mathbb{P}^1) \simeq K(C)$ impliziert. Also ist C über K isomorph zu $\mathbb{P}^1$. ■

FOLGERUNG. *Hat C Geschlecht 0 und besitzt C einen K-rationalen Punkt, so ist C über K isomorph zu $\mathbb{P}^1$. Insbesondere gilt $\#C(K) = \#\mathbb{P}^1(K)$.*

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

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

FOLGERUNG. *Hat C Geschlecht 0, so gilt*

$$\operatorname{Pic}(C) \simeq \mathbb{Z} \quad \textit{und} \quad \operatorname{Pic}^0(C) = 0.$$

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

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

Datei: algku11.tex. Version vom 18.7.2021

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

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

Beweis: Sei H der Divisor eines Hyperebenenschnitts. Er ist über K definiert und hat $\operatorname{grad}(H) = 2m+1$, wenn die Kurve Grad $2m+1$ hat. Sei K_C ein über K definierter kanonischer Divisor. Es gilt $\operatorname{grad}(K_C) = -2$. Dann ist $H + mK_C$ über K definiert mit $\operatorname{grad}(H + mK_C) = 1$, also ist nach unserem Satz C über K isomorph zu $\mathbb{P}^1$. ■

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

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

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

SATZ. *Ist $\widetilde{C} \subseteq \mathbb{P}^n$ eine absolut irreduzible, über K definierte, projektive Kurve ungeraden Grades mit nur endlich vielen Singularitäten, so dass die Desingularisierung C Geschlecht 0 hat, so ist C über K isomorph zu $\mathbb{P}^1$, also gibt es eine Parametrisierung*

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

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

Beweisidee: Man wähle einen über K definierten Hyperebenenschnitt, der keine Singularität enthält. (Braucht man hier eine Voraussetzung über K?) 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 genau einer Singularität, so ist die Desingularisierung isomorph zu $\mathbb{P}^1$. 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:

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

2. Wie kann man sich Kurven vom Geschlecht 0 vorstellen?

Diese Frage beantwortet folgender Satz:

SATZ. *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 $K_C = (df)$ über K definiert. Es gilt

$$\operatorname{grad}(-K_C) = 2 \quad \text{und} \quad \ell(-K_C) = 2 + 1 - 0 + \ell(2K_C) = 3,$$

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

Wir erinnern an eine früher hergeleitete Charakterisierung der Singularität ebener Kegelschnitte, die in jeder Charakteristik gültig ist.

SATZ. *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 nichtsingulär,*
(3) $4a_0a_3a_5 + a_1a_2a_4 - a_2^2a_3 - a_0a_4^2 - a_1^2a_5 \neq 0$.

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. *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 auseinander hervorgehen.*

Natürlich sind projektiv äquivalente Quadriken auch isomorph. Die Umkehrung steht in folgendem Lemma:

LEMMA. *Seien C_1 und C_2 zwei über K definierte nichtsinguläre projektive ebene Quadriken und $\psi : C_1 \to C_2$ ein über K definierter Isomorphismus. Dann gibt es eine Matrix $A = (a_{ij}) \in \mathrm{GL}_3(K)$ mit*

$$\psi((x_0 : x_1 : x_2)) = \left(\sum_j a_{0j}x_j : \sum_j a_{1j}x_j : \sum_j a_{2j}x_j \right).$$

Beweis:

- Zur Unterscheidung verwenden wir auf C_1 die projektiven Koordinaten x_0, x_1, x_2, auf C_2 die projektiven Koordinaten y_0, y_1, y_2.
- Sei H_1 der Hyperebenenschnitt (x_0) auf C_1. Er hat Grad 2 und es gilt $\ell(H_1) = 3$ und
$$\mathcal{L}(H_1) = \overline{K} + \overline{K} \cdot \frac{x_1}{x_0} + \overline{K} \cdot \frac{x_2}{x_0}.$$
- Sei H_2 der Hyperebenenschnitt (y_0) auf C_2. Er hat Grad 2 und es gilt $\ell(H_2) = 3$ und
$$\mathcal{L}(H_2) = \overline{K} + \overline{K} \cdot \frac{y_1}{y_0} + \overline{K} \cdot \frac{y_2}{y_0}.$$
- $\psi^*(H_2)$ ist dann ein effektiver Divisor vom Grad 2 auf C_1 genauso wie H_1. Also sind H_1 und $\psi^*(H_2)$ linear äquivalent, d.h. es gibt eine Funktion $f \in \overline{K}(C_1)$ mit
$$\psi^*(H_2) = H_1 + \mathrm{div}(f).$$
Da H_1 und $\psi^*(H_2)$ über K definiert sind, können wir $f \in K(C_1)$ annehmen.
- Es gilt für $i = 0, 1, 2$
$$\begin{aligned} H_1 + \mathrm{div}(f \cdot \psi^*(\frac{y_i}{y_0})) &= H_1 + \mathrm{div}(f) + \mathrm{div}(\psi^*(\frac{y_i}{y_0})) = \\ &= \psi^*(H_2) + \psi^*(\mathrm{div}(\frac{y_i}{y_0})) = \psi^*\left(H_2 + \mathrm{div}(\frac{y_i}{y_0})\right) \geq 0, \end{aligned}$$
sodass folgt
$$f \cdot \psi^*(\frac{y_i}{y_0}) \in \mathcal{L}(H_1) = \overline{K} \cdot \frac{x_0}{x_0} + \overline{K} \cdot \frac{x_1}{x_0} + \overline{K} \cdot \frac{x_2}{x_0}.$$
Also gibt es Zahlen $a_{ij} \in K$ mit
$$f \cdot \psi^*(\frac{y_i}{y_0}) = \sum_j a_{ij} \frac{x_j}{x_0}.$$
Die $\frac{y_0}{y_0}, \frac{y_1}{y_0}, \frac{y_2}{y_0}$ linear unabhängig sind, ist $A = (a_{ij})$ invertierbar.

- Seien jetzt $p_0, p_1, p_2 \in \overline{K}$ mit $P = (p_0 : p_1 : p_2) \in C_1(\overline{K})$. Wir betrachten den Fall, dass $p_0 \neq 0$ und $f(P) \neq 0$ gilt. Wir setzen P jetzt in die letzte Gleichung ein und erhalten

$$f(P) \cdot \left(\psi^*(\frac{y_i}{y_0})\right)(P) = \frac{1}{p_0} \sum_j a_{ij} p_j,$$

und damit

$$f(P) \cdot (\frac{y_i}{y_0})(\psi(P)) = \frac{1}{p_0} \sum_j a_{ij} p_j.$$

Somit gilt:

$$\begin{aligned}
\psi(P) &= \left(1 : (\frac{y_1}{y_0})(\psi(P)) : (\frac{y_2}{y_0})(\psi(P))\right) = \\
&= \left(f(P) : f(P) \cdot (\frac{y_1}{y_0})(\psi(P)) : f(P) \cdot (\frac{y_2}{y_0})(\psi(P))\right) = \\
&= \left(\frac{1}{p_0}\sum_j a_{0j}p_j : \frac{1}{p_0}\sum_j a_{1j}p_j : \frac{1}{p_0}\sum_j a_{2j}p_j\right) = \left(\sum_j a_{0j}p_j : \sum_j a_{1j}p_j : \sum_j a_{2j}p_j\right).
\end{aligned}$$

Damit gilt also

$$\psi((p_0 : p_1 : p_2)) = \left(\sum_j a_{0j}p_j : \sum_j a_{1j}p_j : \sum_j a_{2j}p_j\right)$$

auf einer offenen Teilmenge, und damit natürlich allgemein. Dies beweist die Behauptung. ■

Die Klassifikation der Kegelschnitte ist ein eigenes Thema, das stark vom Grundkörper abhängt. Wir wollen uns zunächst auf endliche Körper und $\mathbb{Q}$ beschränken.

3. Kurven vom Geschlecht 0 über endlichen Körpern

SATZ. *Jede über $\mathbb{F}_p$ definierte, absolut irreduzible, nichtsinguläre, projektive Kurve C vom Geschlecht 0 ist über $\mathbb{F}_p$ isomorph zu $\mathbb{P}^1$.*

Beweis: C ist über $\mathbb{F}_p$ isomorph zu einem nichtsingulären ebenen Kegelschnitt. Ebene Kegelschnitte haben über $\mathbb{F}_p$ aber immer $\mathbb{F}_p$-rationale Punkte. Damit erhalten wir einen über $\mathbb{F}_p$ definierten Isomorphismus zu $\mathbb{P}^1$. ■

Bis auf $\mathbb{F}_p$-Isomorphie ist also $\mathbb{P}^1$ die einzige über $\mathbb{F}_p$ definierte (absolut irreduzible, nichtsinguläre, projektive) Kurve vom Geschlecht 0.

4. Exkurs: p-adische Zahlen

Dies soll keine systematische Einführung in die p-adischen Zahlen sein, sondern es soll nur kurz ein kleiner Überblick geben werden.
Neben dem üblichen Absolutbetrag $|\cdot|$ gibt es auf $\mathbb{Q}$ für jede Primzahl p einen sogenannten p-adischen Absolutbetrag. Hat $a \in \mathbb{Q}^*$ die Primfaktorzerlegung

$$a = \pm \prod_{p \text{ Primzahl}} p^{v_p(a)},$$

so setzt man

$$|a|_p = \frac{1}{p^{v_p(a)}} \quad \text{und} \quad |0|_p = 0.$$

$|\cdot|_p$ ist eine Funktion $\mathbb{Q} \to \mathbb{R}_{\geq 0}$ mit folgenden Eigenschaften:

- $|a|_p \geq 0$ und $(|a|_p = 0 \iff a = 0)$.
- $|ab|_p = |a|_p |b|_p$.
- $|a+b|_p \leq \max(|a|_p, |b|_p)$. (Daraus folgt die Dreiecksungleichung $|a+b|_p \leq |a|_p + |b|_p$.)

Die Absolutbeträge sind so normiert, dass für alle $a \in \mathbb{Q}^*$ gilt

$$|a| \cdot \prod_p |a|_p = 1.$$

Die Absolutbeträge machen $\mathbb{Q}$ zu einem metrischen Raum. Allerdings ist $\mathbb{Q}$ bezüglich der Absolutbeträge $|\cdot|_p$ (und $|\cdot|$) nicht vollständig, d.h. es gibt Cauchy-Folgen, die nicht konvergieren. Durch Vervollständigung erhält man für den normalen Absolutbetrag die reellen Zahlen $\mathbb{R}$, für $|\cdot|_p$ die Menge der p-adischen Zahlen $\mathbb{Q}_p$. Ebenso wie $\mathbb{R}$ ist auch $\mathbb{Q}_p$ ein Körper. Auch der Absolutbetrag $|\cdot|_p$ setzt sich auf $\mathbb{Q}_p$ fort.

Die Dezimaldarstellung reeller Zahlen zeigt, dass gilt

$$\mathbb{R} = \{\sum_{k=k_0}^{\infty} a_k (\frac{1}{10})^k : a_k \in \{0, 1, \ldots, 9\}, k_0 \in \mathbb{Z}\}.$$

Überlegung: Gibt man sich $a_k \in \{0, 1, \ldots, p-1\}$ für alle $k \geq 0$ beliebig vor, so bildet die Folge der Partialsummen

$$\left(\sum_{k=0}^{n} a_k p^k\right)_{n \in \mathbb{N}}$$

eine Cauchy-Folge bzgl. $|\cdot|_p$, denn für $m > n$ gilt

$$\left|\sum_{k=0}^{m} a_k p^k - \sum_{k=0}^{n} a_k p^k\right|_p = \left|\sum_{k=n+1}^{m} a_k p^k\right|_p = |p|_p^{n+1} \left|\sum_{k=n+1}^{m} a_k p^{k-n-1}\right|_p \leq |p|_p^{n+1} = \frac{1}{p^{n+1}},$$

also existiert der Grenzwert

$$\sum_{k=0}^{\infty} a_k p^k = \lim_{n \to \infty} \left(\sum_{k=0}^{n} a_k p^k\right)$$

in $\mathbb{Q}_p$.

Man erhält dann

$$\mathbb{Q}_p = \{\sum_{k=k_0}^{\infty} a_k p^k : a_k \in \{0, 1, \ldots, p-1\}, k_0 \in \mathbb{Z}\}.$$

(Die p-adische Entwicklung $\alpha = \sum_{k=k_0}^{\infty} a_k p^k$ einer Zahl $\alpha \in \mathbb{Q}_p$ ist eindeutig bestimmt.)
SAGE stellt mit `K=Qp(p)` den Körper $\mathbb{Q}_p$ bereit, mit `K(a)` erhält man die p-adische Entwicklung einer Zahl. Beispielsweise liefern `K=Qp(7)` und `K(37/35)` die 7-adische Entwicklung von $\frac{37}{35}$:

$$\frac{37}{35} = 6 \cdot 7^{-1} + 3 + 7 + 4 \cdot 7^2 + 5 \cdot 7^3 + 2 \cdot 7^4 + 7^5 + 4 \cdot 7^6 + 5 \cdot 7^7 + 2 \cdot 7^8 + 7^9 + 4 \cdot 7^{10} + 5 \cdot 7^{11} + 2 \cdot 7^{12} + 7^{13} + 4 \cdot 7^{14} + 5 \cdot 7^{15} + 2 \cdot 7^{16} + 7^{17} + 4 \cdot 7^{18} + O(7^{19})$$

Die Menge der **ganzen p-adischen Zahlen** ist

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p \leq 1\}.$$

$\mathbb{Z}_p$ ist ein diskreter Bewertungsring mit der Bewertung $v_p(a)$, sodass gilt

$$|a|_p = p^{-v_p(a)}.$$

$\mathbb{Z}$ ist eine dichte Teilmenge von $\mathbb{Z}_p$ und es gilt

$$\mathbb{Z}_p = \{\sum_{k=0}^{\infty} a_k p^k : a_k \in \{0, 1, \ldots, p-1\}\}.$$

Man kann modulo p^n rechnen:

$$\sum_{k=0}^{\infty} a_k p^k \equiv a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} \bmod p^n.$$

Will man in $\mathbb{R}$ eine Gleichung $f(x) = 0$ lösen, so besteht die Idee des **Newton-Verfahrens** darin, mit einer Näherungslösung x_0, d.h. $f(x_0) \approx 0$, zu beginnen, dann den Schnittpunkt der Tangente des Graphen

von f in x_0 mit der x-Achse als neuen Näherungswert x_1 zu verwenden, und dieses dann zu iterieren [**Forster1**, S.199-203].

Die gleiche Idee kann man auch in $\mathbb{Q}_p$ bzw. $\mathbb{Z}_p$ verwenden. Sei $f(x) \in \mathbb{Z}[x]$ ein Polynom in einer Veränderlichen. Für $x_0 \in \mathbb{Z}$ gilt:

$$f(x_0) \equiv 0 \bmod p^n \iff p^n \mid f(x_0) \iff \frac{f(x_0)}{p^n} \in \mathbb{Z} \iff$$
$$\iff \left|\frac{f(x_0)}{p^n}\right|_p \leq 1 \iff |f(x_0)|_p \leq |p|_p^n = \frac{1}{p^n}.$$

Eine Lösung der Gleichung $f(x) = 0$ modulo p^n approximiert also eine p-adische Nullstelle von $f(x)$. Dies lässt sich auch präzisieren. Beispielsweise gilt folgender Satz:

SATZ. *Ist $f(x) \in \mathbb{Z}[x]$ und $x_0 \in \mathbb{Z}$ mit*

$$f(x_0) \equiv 0 \bmod p \quad \textit{und} \quad v_p(f'(x_0)) = 0,$$

so existiert eine Zahl $\widetilde{x} \in \mathbb{Z}_p$ mit $f(\widetilde{x}) = 0$ und es gilt $\widetilde{x} \equiv x_0 \bmod p$. Die angegebenen Bedingungen lassen sich auch in der Form

$$|f(x_0)|_p < 1 \quad \textit{und} \quad |f'(x_0)|_p = 1$$

schreiben.

Genaueres findet sich bei [**Serre**, S.14-15]. Aussagen dieser Art sind auch unter dem Namen **Hensels Lemma** bekannt.

5. Kurven vom Geschlecht 0 über $\mathbb{Q}$ - Hilbert-Symbol

LEMMA. *Wird die ebene projektive Quadrik C über $\mathbb{Q}$ definiert durch $f = b_0x_0^2+b_1x_1^2+b_2x_2^2$, sind b_0, b_1, b_2 paarweise teilerfremde, quadratfreie, ganze Zahlen, ist p eine ungerade Primzahl mit*

$$p \mid b_0 \quad \textit{und} \quad \left(\frac{-b_1b_2}{p}\right) = -1,$$

so gilt

$$C(\mathbb{Q}_p) = \emptyset.$$

Beweis: Angenommen, es gibt $(y_0, y_1, y_2) \in \mathbb{Q}_p^3 \setminus \{(0,0,0)\}$ mit $f(y_0, y_1, y_2) = 0$. Nach Multiplikation oder Division mit einer geeigneten Potenz von p können wir

$$(y_0, y_1, y_2) \in \mathbb{Z}_p^3 \quad \text{und} \quad \min(v_p(y_0), v_p(y_1), v_p(y_2)) = 0$$

annehmen. Aus $b_0y_0^2 + b_1y_1^2 + b_2y_2^2 = 0$ folgt mit $p \mid b_0$ modulo p

$$b_1y_1^2 + b_2y_2^2 \equiv 0 \bmod p,$$

und damit

$$(b_2y_2)^2 \equiv -b_1b_2y_1^2 \bmod p.$$

Wegen $\left(\frac{-b_1b_2}{p}\right) = -1$ muss $y_1 \equiv 0 \bmod p$ gelten. Mit $p \mid b_0$ folgt dann aus der ursprünglichen Gleichung $p \mid y_2$, und damit

$$p^2 \mid b_1y_1^2 + b_2y_2^2, \quad \text{also} \quad p^2 \mid b_0y_0^2.$$

Da p die Zahl b_0 nur einmal teilt, folgt $p \mid y_0$. Damit erhält man den Widerspruch $\min(v_p(y_0), v_p(y_1), v_p(y_2)) \geq 1$. Die Annahme ist also falsch, es folgt die Behauptung. ■

LEMMA. *Eine ebene projektive Quadrik C werde gegeben durch $f = b_0x_0^2 + b_1x_1^2 + b_2x_2^2$ mit ganzen, quadratfreien, paarweise teilerfremden Zahlen $b_0, b_1, b_2 \in \mathbb{Z} \setminus \{0\}$. Sei p eine ungerade Primzahl. Gilt*

$$p \nmid b_0b_1b_2 \quad \textit{oder} \quad \left(p \mid b_0 \textit{ und } \left(\frac{-b_1b_2}{p}\right) = 1\right),$$

so ist

$$C(\mathbb{Q}_p) \neq \emptyset.$$

Beweis: Betrachten wir das Polynom f modulo p, so erhalten wir eine Kurve $\overline{C}$ über $\mathbb{F}_p$. Im Fall $p \nmid b_0b_1b_2$ ist die Kurve nichtsingulär und es gilt $\#\overline{C}(\mathbb{F}_p) = p+1$, im Fall $p \mid b_0$ und $\left(\frac{-b_1b_2}{p}\right) = 1$ zerfällt $\overline{C}$ über $\mathbb{F}_p$ in zwei Geraden und $\#\overline{C}(\mathbb{F}_p) = 2p+1$, insbesondere gibt es auch hier über $\mathbb{F}_p$ definierte nichtsinguläre Punkte. In jedem Fall finden wir also $(y_0, y_1, y_2) \in \mathbb{Z}^3 \subseteq \mathbb{Z}_p^3$ mit

$$f(y_0, y_1, y_2) \equiv 0 \bmod p \quad \text{und} \quad (\frac{\partial f}{\partial x_0}(y_0, y_1, y_2), \frac{\partial f}{\partial x_1}(y_0, y_1, y_2), \frac{\partial f}{\partial x_2}(y_0, y_1, y_2)) \not\equiv (0,0,0) \bmod p.$$

Nach [**Serre**, S.14, Theorem 1] gibt es dann Zahlen $\widetilde{y}_0, \widetilde{y}_1, \widetilde{y}_2 \in \mathbb{Z}_p$ mit

$$f(\widetilde{y}_0, \widetilde{y}_1, \widetilde{y}_2) = 0 \quad \text{und} \quad \widetilde{y}_i \equiv y_i \bmod p \text{ für } i = 0,1,2.$$

Dann ist $(\widetilde{y}_0 : \widetilde{y}_1 : \widetilde{y}_2) \in C(\mathbb{Q}_p)$ und die Behauptung folgt. ■

Bemerkung: [**Serre**, S.14, Theorem 1] enthält leider den Schreibfehler $0 < 2k < n$. In der französischen Aussage [**Serre 1970**, S.28-29, Théorème 1] steht richtig $0 \leq 2k < n$.

Damit können wir den Satz von Legendre nun umformulieren:

Satz (Satz von Legendre, 2. Version). *Sei C eine absolut irreduzible, nichtsinguläre, projektive, ebene Quadrik, die über $\mathbb{Q}$ definiert ist. Dann gilt:*

$$C(\mathbb{Q}) \neq \emptyset \quad \Longleftrightarrow \quad C(\mathbb{R}) \neq \emptyset \text{ und } C(\mathbb{Q}_p) \neq \emptyset \text{ für alle ungeraden Primzahlen } p.$$

Erstaunlicherweise wird im vorangegangenen Satz die Primzahl 2 nicht erwähnt.

Das Hilbert-Symbol [**Serre**, S.19-26, Chapter III]. Im Folgenden schreiben wir $\mathbb{Q}_\infty$ für $\mathbb{R}$. Für $v = \infty$ oder $v = p$ und $a, b \in \mathbb{Q}_v^*$ wird das **Hilbert-Symbol** $(a,b)_v$ von a, b bezüglich $\mathbb{Q}_v$ definiert durch

$$(a,b)_v = \begin{cases} 1, & \text{falls } ax^2 + by^2 = z^2 \text{ hat eine Lösung } (x,y,z) \in \mathbb{Q}_v^3 \setminus \{(0,0,0)\}, \\ -1 & \text{sonst.} \end{cases}$$

Man kann das Hilbert-Symbol ausrechnen [**Serre**, S.20, Theorem 1]:

Satz. (1) *Für $a, b \in \mathbb{R}^*$ gilt*

$$(a,b)_\infty = \begin{cases} 1, & \text{falls } a > 0 \text{ oder } b > 0, \\ -1, & \text{falls } a < 0 \text{ und } b < 0. \end{cases}$$

(2) *Seien $a, b \in \mathbb{Q}_p^*$. Zerlegt man*

$$a = p^\alpha u, \quad b = p^\beta v \quad \text{mit} \quad v_p(u) = v_p(v) = 0,$$

so gilt im Fall $p > 2$ (mit den Legendre-Symbolen $\left(\frac{u}{p}\right)$ und $\left(\frac{v}{p}\right)$)

$$(a,b)_p = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha$$

und im Fall $p = 2$

$$(a,b)_2 = (-1)^{\varepsilon(u)\varepsilon(v) + \alpha\omega(v) + \beta\omega(u)}.$$

Dabei sind ε und ω die Funktionen

$$\varepsilon(u) = \frac{u-1}{2} \bmod 2 \quad \text{und} \quad \omega(u) = \frac{u^2-1}{8} \bmod 2.$$

Bemerkung: Für $a, b \in \mathbb{Q}^*$ gilt für eine ungerade Primzahl p

$$(a,b)_p = 1, \text{ falls } v_p(a) = v_p(b) = 0 \text{ ist.}$$

Da in der Primfaktorzerlegung von a und b nur endlich viele Primzahlen vorkommen, ist

$$\{p \text{ Primzahl} : (a,b)_p = -1\}$$

eine endliche Menge.

Bemerkung: SAGE berechnet das Hilbert-Symbol $(a,b)_p$ mit dem Befehl `hilbert_symbol(a,b,p)`, das Hilbert-Symbol $(a,b)_\infty$ mit dem Befehl `hilbert_symbol(a,b,-1)`.

Bemerkung: Jede über $\mathbb{Q}$ definierte nichtsinguläre projektive ebene Quadrik C kann nach Koordinatenwechsel über $\mathbb{Q}$ durch eine Gleichung der Form

$$f = ax_0^2 + bx_1^2 - x_2^2$$

beschrieben werden. Dann gilt also

$$C(\mathbb{Q}_p) = \emptyset \quad \Longleftrightarrow \quad (a,b)_p = -1.$$

Beispiele: Wir betrachten eine nichtsinguläre Quadrik C über $\mathbb{Q}$, die durch ein Polynom $f = b_0x_0^2 + b_1x_1^2 + b_2x^2$ gegeben ist mit $b_0, b_1, b_2 \in \mathbb{Z} \setminus \{0\}$, quadratfrei, paarweise teilerfremd. Es gilt:

$$b_0x_0^2 + b_1x_1^2 + b_2x_2^2 = 0 \quad \Longleftrightarrow \quad -b_0b_2x_0^2 - b_1b_2x_1^2 = (b_2x_2)^2,$$

die Quadrik lässt sich also auch durch

$$(-b_0b_2)x^2 + (-b_1b_2)y^2 = z^2$$

beschreiben. Wir betrachten daher für eine ungerade Primzahl p das Hilbert-Symbol

$$(-b_0b_2, -b_1b_2)_p.$$

(1) **Fall $p \nmid b_0b_1b_2$:** Aus $v_p(-b_0b_2) = v_p(-b_1b_2) = 0$ folgt sofort

$$(-b_0b_2, -b_1b_2)_p = 1.$$

(2) **Fall $p \mid b_0b_1b_2$:** O.E. betrachten wir den Fall $p \mid b_0$. Wir zerlegen

$$-b_0b_2 = p^1u, \quad -b_1b_2 = p^0v, \quad \text{also} \quad \alpha = 1, \quad \beta = 0.$$

Wegen $\beta = 0$ und $\alpha = 1$ erhalten wir

$$(-b_0b_2, -b_1b_2)_p = \left(\frac{-b_1b_2}{p}\right).$$

Dieses Legendre-Symbol mussten wir im Satz von Legendre betrachten.

Für das globale Verhalten ist folgender Satz wichtig [**Serre**, S.23, Theorem 3 (Hilbert)]:

Satz (Produktformel für das Hilbert-Symbol). *Sind $a, b \in \mathbb{Q}^*$, so gilt $(a,b)_p = 1$ für fast alle Primzahlen und*

$$(a,b)_\infty \cdot \prod_p (a,b)_p = 1.$$

Bemerkungen:

(1) Aus der Produktformel für das Hilbert-Symbol folgt

$$(a,b)_2 = (a,b)_\infty \cdot \prod_{p \neq 2} (a,b)_p.$$

Dies erklärt, warum wir beim Satz von Legendre die Primzahl 2 nicht gebraucht haben.

(2) Wir können die Produktformel auch nach $(a,b)_\infty$ auflösen:

$$(a,b)_\infty = \prod_p (a,b)_p.$$

Für eine über $\mathbb{Q}$ definierte nichtsinguläre projektive ebene Quadrik C definieren wir

$$\Psi(C) = \{p \text{ Primzahl} : C(\mathbb{Q}_p) = \emptyset\}.$$

Wird C durch eine Gleichung $ax_0^2 + bx_1^2 = x_2^2$ beschrieben, so ist also

$$\Psi(C) = \{p \text{ Primzahl} : (a,b)_p = -1\}.$$

Wegen der Produktformel für das Hilbert-Symbol folgt dann

$$C(\mathbb{R}) \begin{cases} \neq \emptyset, & \text{falls } \#\Psi(C) \text{ gerade,} \\ = \emptyset, & \text{falls } \#\Psi(C) \text{ ungerade.} \end{cases}$$

Wir können nun den Satz von Legendre auch so formulieren:

$$C(\mathbb{Q}) \neq \emptyset \quad \Longleftrightarrow \quad \Psi(C) = \emptyset.$$

Bemerkung: SAGE berechnet für eine nichtsinguläre Quadrik C der Form $ax_0^2 + bx_1^2 - x_2^2$ das Produkt

$$\prod_{p \in \Psi(C)} p$$

mit dem Befehl `hilbert_conductor(a,b)`.

Satz. *Zwei über $\mathbb{Q}$ definierte nichtsinguläre projektive ebene Quadriken C_1 und C_2 sind genau dann isomorph über $\mathbb{Q}$, wenn gilt $\Psi(C_1) = \Psi(C_2)$.*

Leider kenne ich keinen direkten Beweis dieses Satzes. Ein Beweis benutzt Quaternionenalgebren. (Der Zusammenhang zwischen Kegelschnitten und Quaternionenalgebren wird in [**Gille-Szamuely**, Abschnitte 1.3 (The associated conic) und 1.4 (A Theorem of Witt)] behandelt.)

Beispiele: Wir haben zufällig $a_0, \ldots, a_5 \in \mathbb{Z}$ (mit $|a_i| \leq 10$) gewählt, dazu die durch $f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$ definierte Quadrik C betrachtet - nur im nichtsingulären Fall -, die Quadrik zu $ax_0^2 + bx_1^2 = x_2^2$ diagonalisiert und dann $\Psi(C)$ berechnet:

$(a_0, a_1, a_2, a_3, a_4, a_5)$	(a, b)	$\Psi(C)$
$(-7, -6, 7, -9, 1, -3)$	$(-21, -14)$	$\{2\}$
$(5, -9, 7, -2, 8, 5)$	$(-55, 55)$	$\emptyset$
$(0, 0, -4, 1, 0, -9)$	$(-1, 1)$	$\emptyset$
$(-2, -9, -10, 6, 2, -7)$	$(-126678, 982)$	$\emptyset$
$(3, -2, 3, 6, 7, -4)$	$(26265, 1545)$	$\{5, 103\}$
$(-1, 10, 0, 0, 0, -8)$	$(-2, 2)$	$\emptyset$
$(-6, -5, 8, 4, 5, -8)$	$(-993, 993)$	$\emptyset$
$(8, 4, 10, 9, -9, 9)$	$(-510, -30)$	$\{5\}$
$(-2, 10, 2, -6, 4, 9)$	$(2158, -166)$	$\{2, 83\}$
$(-8, -5, -5, 6, -9, -1)$	$(-1085, 5)$	$\{5, 7\}$
$(2, -10, -8, -6, 0, -7)$	$(26270, -710)$	$\{2, 5\}$
$(7, 1, -2, 10, -5, 6)$	$(-318773, -10283)$	$\{13\}$
$(-1, -7, 9, 2, 5, -5)$	$(9519, -167)$	$\emptyset$
$(2, -5, 9, 7, -8, -4)$	$(3162, 102)$	$\{17, 3\}$
$(-7, 8, -5, 10, 5, -1)$	$(-41538, 483)$	$\{3, 23\}$
$(7, 9, -1, -2, -2, 7)$	$(-927353, 6769)$	$\emptyset$
$(7, 1, -5, 2, -10, -6)$	$(15862, 7210)$	$\{5, 103\}$
$(8, 1, 10, -2, -9, -4)$	$(-9035, 139)$	$\emptyset$
$(10, 1, -8, 5, 7, 4)$	$(1393, 7)$	$\emptyset$

$(a_0, a_1, a_2, a_3, a_4, a_5)$	(a, b)	$\Psi(C)$
$(8, 3, 10, -3, -5, 2)$	$(-546, 130)$	$\emptyset$
$(-3, 6, 8, -10, -4, 0)$	$(217, 93)$	$\emptyset$
$(9, -2, 6, 6, 8, -2)$	$(4346, 82)$	$\{41, 2\}$
$(-10, -3, 9, 5, 8, -7)$	$(-2145, 3705)$	$\{19, 3\}$
$(-8, -1, -4, 3, -2, 3)$	$(6790, -70)$	$\{5, 7\}$
$(-6, 0, 2, 8, -4, -5)$	$(-2, 6)$	$\emptyset$
$(4, 9, -10, 10, -1, 6)$	$(8690, 110)$	$\emptyset$
$(-3, -7, -9, 9, 9, 10)$	$(701319, -4467)$	$\emptyset$
$(-10, -6, 1, 3, 2, 5)$	$(11778, -302)$	$\emptyset$
$(-4, 1, -4, 6, -9, 4)$	$(3007, -31)$	$\emptyset$
$(5, 4, -2, 2, 7, -9)$	$(70, 105)$	$\emptyset$
$(-8, 5, 2, 7, 7, 10)$	$(63993, -257)$	$\emptyset$
$(-8, -8, 5, 10, -3, 10)$	$(11694, -1949)$	$\emptyset$
$(1, -4, 9, 4, 4, -7)$	$(-109, 1)$	$\emptyset$
$(-9, 9, 2, -8, -2, -1)$	$(-161, -7)$	$\{7\}$
$(5, -6, -1, -6, 7, 8)$	$(-39, 1)$	$\emptyset$
$(10, -7, 3, -4, -6, 6)$	$(-6270, 30)$	$\{11, 3\}$
$(-1, 0, 1, 4, 6, -3)$	$(-5, 5)$	$\emptyset$
$(0, -5, 3, 1, -10, 2)$	$(91, -91)$	$\emptyset$
$(-2, -4, 3, 1, -1, -9)$	$(-663, 442)$	$\{17, 13\}$
$(4, -5, 9, 2, -9, 8)$	$(7, 1)$	$\emptyset$
$(-7, -5, 8, 9, 2, 4)$	$(17174, -62)$	$\{2, 31\}$
$(-4, -2, 5, -9, 2, 5)$	$(32235, 921)$	$\emptyset$
$(10, 8, -6, 9, 6, -1)$	$(58645, 3170)$	$\{2, 317\}$
$(7, 1, 2, 3, -5, -1)$	$(830, 10)$	$\{2, 5\}$
$(7, 1, 4, -1, 2, 9)$	$(-53795, 1855)$	$\emptyset$
$(1, 8, 3, -1, -6, 5)$	$(-8687, 511)$	$\{73, 7\}$
$(2, -4, -3, 3, -7, -8)$	$(273, 546)$	$\{13, 7\}$
$(5, -3, -1, 0, -10, 0)$	$(-106, 106)$	$\emptyset$
$(7, 4, 8, 8, 1, -1)$	$(63245, 4865)$	$\{139, 5\}$
$(8, 3, -8, -4, -9, 4)$	$(-49594, 362)$	$\emptyset$

Bei den Beispielen fällt auf, dass die Fälle mit $\psi(C) = \emptyset$ recht häufig sind. (Dies sind genau die Fälle mit $C(\mathbb{Q}) \neq \emptyset$.)

Bemerkungen:

(1) $\Psi(C)$ ist eine endliche Menge von Primzahlen. Man kann umgekehrt zeigen, dass es zu jeder endlichen Menge $\widetilde{P}$ von Primzahlen eine Kurve C mit $\Psi(C) = \widetilde{P}$ gibt.

(2) Ist $\widetilde{P} = \{p_1, \ldots, p_r\}$ eine endliche Menge von Primzahlen, setzt man $d = p_1 \ldots p_r$ so liefert der SAGE-Befehl `hilbert_conductor_inverse(d)` ein Zahlenpaar $(a, b) \in \mathbb{Z}^2$, sodass für die durch $ax_0^2 + bx_1^2 = x_2^2$ definierte Kurve C gilt $\Psi(C) = \widetilde{P}$. Beispielsweise erhält man für $\widetilde{P} = \{2, 3, 5, 7, 11\}$ die Kurve $-22x_0^2 + 210x_1^2 = x_2^2$.

(3) Die $\mathbb{Q}$-Isomorphieklassen der über $\mathbb{Q}$ definierten, absolut irreduziblen, nichtsingulären, projektiven Kurven vom Geschlecht 0 stehen also in Bijektion zu den endlichen Teilmengen der Menge der Primzahlen.

Bemerkung: Sind C_1, C_2 zwei nichtsinguläre ebene Quadriken mit $\Psi(C_1) = \Psi(C_2)$, so gibt es also einen über $\mathbb{Q}$ definierten Koordinatenwechsel, der C_1 in C_2 überführt. Wie findet man einen solchen?
Hier ist eine (nicht ganz ausgereifte) Idee:

(1) Wir transformieren C_1 auf eine Gleichung $ax_0^2 + bx_1^2 - abx_2^2 = 0$ und C_2 auf eine Gleichung $\widetilde{a}y_0^2 - \widetilde{y}_1^2 - \widetilde{a}\widetilde{b}y_2^2 = 0$.

(2) Die Zahlen $a, b \in \mathbb{Q}^*$ definieren die Quaternionen-Algebra $Q(a, b)$ mit $\mathbb{Q}$-Basis $1, i, j, k$, d.h.

$$Q(a, b) = \mathbb{Q} \cdot 1 + \mathbb{Q} \cdot i + \mathbb{Q} \cdot j + \mathbb{Q} \cdot k,$$

wobei gilt

$$i^2 = a, \quad j^2 = b, \quad ji = -ij, \quad k = ij, \quad k^2 = -ab.$$

(3) Da C_1 über $\mathbb{Q}$ isomorph zu C_2 sein sollte, sind nach dem Satz von Witt [**Gille-Szamuely**, Theorem 1.4.2 (Witt)] die Quaternionenalgebren $Q(a,b)$ und $Q(\widetilde{a},\widetilde{b})$ isomorph. Es sollte also Elemente $\widetilde{i},\widetilde{j} \in Q(a,b)$ geben mit

$$\widetilde{i}^2 = \widetilde{a}, \quad \widetilde{j}^2 = \widetilde{b}, \quad \widetilde{j}\widetilde{i} = -\widetilde{i}\widetilde{j}.$$

Wir setzen dann

$$\widetilde{k} = \widetilde{i}\widetilde{j}.$$

(Es folgt $\widetilde{k}^2 = -\widetilde{a}\widetilde{b}$.) Dann gibt es $a_{ij} \in \mathbb{Q}$ mit

$$\begin{pmatrix} \widetilde{i} \\ \widetilde{j} \\ \widetilde{k} \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} i \\ j \\ k \end{pmatrix}.$$

(4) Definieren wir einen Koordinatenwechsel durch

$$\begin{pmatrix} x_0 & x_1 & x_2 \end{pmatrix} = \begin{pmatrix} y_0 & y_1 & y_2 \end{pmatrix} \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{pmatrix},$$

so gilt

$$ax_0^2 + bx_1^2 - abx_2^2 = \widetilde{a}y_0^2 + \widetilde{b}y_1^2 - \widetilde{a}\widetilde{b}y_2^2,$$

wie man durch Einsetzen nachrechnen kann. Damit haben einen gesuchten Isomorphismus gefunden. (Natürlich bleibt die Frage, wie man $\widetilde{i},\widetilde{j}$ praktisch finden kann.)