Hasse-Minkowski für ebene quadratische Formen

Seien $a, b \in \mathbb{Q}^\times$. Wir betrachten die Gleichungen

$$aX^2 + bY^2 = 1 \tag{1}$$

bzw.

$$aX^2 + bY^2 = Z^2. \tag{2}$$

Wir erinnern:

Proposition 1. *Äquivalent sind:*

1. $aX^2 + bY^2 = 1$ *hat eine Lösung* $(x, y) \in \mathbb{Q}^2$
2. $aX^2 + bY^2 = Z^2$ *hat eine Lösung* $(0, 0, 0) \neq (x, y, z) \in \mathbb{Q}^3$.

Proof. Ist (x, y) eine Lösung von (1), so setze $z = 1$. Ist umgekehrt (x, y, z) eine Lösung von (2), und ist $z \neq 0$, so ist $(x/z, y/z)$ eine Lösung von (1). Ist $z = 0$ und o.E. $x \neq 0$, so betrachtet man $a = \frac{z^2}{x^2} - b\frac{y^2}{x^2}$ bzw. die Quadrik $a = u^2 - bv^2$, die dann nach Voraussetzung eine rationale Lösung hat. Damit existieren wegen der Parametrisierung durch $\mathbb{Q}$ schon aber unendlich viele Lösungen, d.h. es muss eine mit $u \neq 0$ existieren, sodass $(1/u^2, v^2/u^2)$ eine Lösung von 1. ist. □

Definition 2. *Sei* $p \in \mathbb{P} \cup \{\infty\}$. *Wir definieren*

$$(a, b)_p = 1 \iff \exists x, y \in \mathbb{Q}_p : (x, y) \text{ ist eine Lösung von } (1)$$

und $(a, b)_p = -1$ *sonst (beachte:* $\mathbb{Q}_\infty = \mathbb{R}$*).*

Ziel ist es, folgenden Satz zu zeigen:

Theorem 3. *(1) hat eine Lösung in* $\mathbb{Q}$ *genau dann, wenn (1) eine Lösung in* $\mathbb{Q}_p$ *hat für alle* $p \in \mathbb{P} \cup \infty$.

Wir benötigen folgende Eigenschaften von $(-, -)_p$:

Theorem 4.

1. $(a, bc^2)_p = (a, b)_p = (ac^2, b)_p$,
2. $(a, b)_p = (b, a)_p$,
3. $(a, -a)_p = 1$ *und* $(a, 1 - a)_p = 1$ *falls* $a \neq 1$.
4. $(aa', b) = (a, b)$ *falls* $(a', b) = 1$.

Wir fixieren einen algebraischen Abschluss $\overline{\mathbb{Q}_p}$ und eine Lösung $\sqrt{b} \in \overline{\mathbb{Q}_p}$ von $X^2 - b$. Dann ist $K = \mathbb{Q}_p(\sqrt{b})$ eine quadratische galoissche Erweiterung (in dem Fall, dass b nicht schon ein Quadrat ist) von $\mathbb{Q}_p$ mit Galoisgruppe $G = \mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/2\mathbb{Z} = \{\mathrm{id}, \sigma\}$, wobei $\sigma : \sqrt{b} \mapsto -\sqrt{b}$. Wir betrachten in jedem Fall

$$N_b : K^\times \longrightarrow \mathbb{Q}_p^\times, \quad x \longmapsto \prod_{\tau \in G} \tau(x).$$

Ist b kein Quadrat in $\mathbb{Q}_p^\times$, so sei $x = u + \sqrt{b}v \in K^\times$, und es gilt also

$$x \cdot \sigma(x) = (u + \sqrt{b}v)(u - \sqrt{b}v) = u^2 - bv^2.$$

Daher definieren wir die Gruppe $N_b := N_b(K^\times)$, die gleich $\{x \in \mathbb{Q}_p^\times | \ \exists u, v \in \mathbb{Q}_p : x = u^2 - bv^2\}$ ist, falls b kein Quadrat ist, und gleich $\mathbb{Q}_p^\times$ sonst.

Theorem 5. $(a, b)_p = 1 \iff a \in N_b \iff b \in N_a$.

Proof. Ist $b = c^2$ für $c \in \mathbb{Q}_p$, so löst $(0, 1, c)$ die Gleichung (2), d.h. $(a, b)_p = 1$ für alle $a \in \mathbb{Q}_p^\times$ genau dann, wenn $a \in N_b = \mathbb{Q}_p^\times$.

Sei b also kein Quadrat. Ist $a = u^2 - bv^2$, so ist $(1, v, u)$ eine Lösung von (2). Ist $(a, b)_p = 1$, und (x, y, z) eine Lösung von (2), so gilt $x \neq 0$, da sonst b ein Quadrat wäre. D.h. $a = \frac{z^2}{x^2} - b\frac{y^2}{x^2}$, d.h. $a \in N_b$. □

Proof. (Theorem 4) 1. und 2. sind klar. Für 3. sieht man, dass $(1, 1, 0)$ eine Lösung von $aX^2 - aY^2 = Z^2$ ist, und dass $(1, 1, 1)$ eine Lösung von $aX^2 + (1 - a)Y^2 = Z^2$ ist.

4.: Ist $(a', b) = 1$, so gilt $a' \in N_b$, d.h. $a'a \in N_b \iff a \in N_b$, da N_b Untergruppe von $\mathbb{Q}_p^\times$ ist. D.h. $(aa', b) = 1 \iff (a, b) = 1$. □

Also faktorisiert das Hilbert-Symbol auf folgende Weise:

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \times \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \to \{\pm 1\}.$$

Aus dem letzten Vortrag wissen wir aber, dass (wenn $p \neq 2, \infty$)

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \oplus \mathbb{Z}_p^\times \cong \mathbb{Z} \oplus \mathbb{F}_p^\times \oplus (1 + p\mathbb{Z}_p) \cong \mathbb{Z} \oplus \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}_p,$$

sodass diese Identifizierung einen Isomorphismus von Gruppen

$$\varphi : \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

induziert. Sei $w \in \mathbb{Z}_p^\times$ ein quadratischer Nichtrest modulo p. Wir behaupten, dass $1, p, w, pw$ ein Vertetersystem von $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ ist:

$$1 = p^0 \cdot 1 \mapsto (0, 0), \ p = p^1 \cdot 1 \mapsto (1, 0), \ w = p^0 \cdot w \mapsto (0, 1), \ pw \mapsto (1, 0) + (0, 1) = (1, 1).$$

Proposition 6. *Sei $p \neq 2, \infty$. Seien $u, v \in \mathbb{Z}_p^\times$. Es gilt:*

1. $(p,u)_p = \left(\frac{u}{p}\right) = 1$, *falls* $u \mod p \in \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ *quadratischer Rest ist, und* -1 *sonst.*

2. $(u,v)_p = 1$.

Proof. Zu 1.: Sei u ein Quadrat in $\mathbb{Z}_p^\times$. Dann gilt sicher $\left(\frac{u}{p}\right) = 1$, da u mod p immer noch ein Quadrat ist. Andererseits ist $(0,1,1)$ eine Lösung von $pX^2 + Y^2 = Z^2$, d.h. $(p,u)_p = 1$. Ist u kein Quadrat, so gilt $\varphi(u) = (0,1) = \varphi(w)$, d.h. $uw^{-1} \in (\mathbb{Z}_p^\times)^2$, also $u = c^2 w$ für ein $c \in \mathbb{Z}_p^\times$. Wir müssen also nur den Fall $u = w$ noch betrachten, und können annehmen, dass u ein quadratischer Nichtrest mod p ist, d.h. $\left(\frac{u}{p}\right) = -1$. Angenommen, $pX^2 + uY^2 = Z^2$ hätte eine Lösung $(x,y,z) \in \mathbb{Q}_p^3$. Dann können wir durch Multiplikation einer p-Potenz erreichen, dass $y, z \in \mathbb{Z}_p^\times$ und $x \in \mathbb{Z}_p$: es gibt $x', y', z' \in \mathbb{Z}_p^\times$, sodass

$$p(p^k x')^2 + u(p^l y')^2 = (p^m z')^2 \iff p^{2k+1}x'^2 + up^{2l}y'^2 = p^{2m}z'^2, d.h.$$

$\mathrm{ord}_p(L.S) = 2l = \mathrm{ord}_p(R.S)$, sodass man durch p^{2m} teilen kann. Mod p bedeutet das, dass u quadratischer Rest ist, Widerspruch, sodass $(p,u) = -1$ folgen muss.

Zu 2.: Ist u oder v ein Quadrat, so gilt die Behauptung. Wir müssen also den Fall $u = v = w$ bzw. die Gleichung $X^2 + Y^2 = u^{-1}$ betrachten. Wir wissen, dass es $(p+1)/2$ viele Quadrate in $\mathbb{F}_p$ gibt: $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ hat $(p-1)/2$ Quadrate, und mit der Null macht das $(p-1)/2+1 = (p+1)/2$. Daher bestehen $\{x^2 \mod p |\ x \in \mathbb{Z}\}$ und $\{u^{-1} - y^2 \mod p |\ y \in \mathbb{Z}_p\}$ jeweils aus $(p+1)/2$ Elementen, was impliziert, dass $(x,y) \in \mathbb{Z}_p$ existieren, sodass $x^2 + y^2 = u^{-1} \mod p$. O.E. gelte $v_p(x) = 0$. Dann gilt für $f(X) = X^2 + y^2 - u^{-1} \in \mathbb{Z}_p[X]$: $f(x) = 0 \mod p$ und $f'(x) = 2x \neq 0 \mod p$. Mit dem Hensel'schen Lemma existiert ein $\alpha \in \mathbb{Z}_p$, sodass $f(\alpha) = 0$, d.h. (α, y) ist Lösung $uX^2 + uY^2 = 1$, sodass $(u,u)_p = 1$. □

Bevor wir das Hensel'sche Lemma beweisen, benötigen wir die Taylorentwicklung für Polynome: sind $x, y \in K$ für einen Körper der Charakteristik 0 und $f(X) \in K[X]$, so gilt

$$f(x+y) = f(x) + f'(x)y + \frac{1}{2!}f''(x)y^2 + \frac{1}{3!}f'''(x)y^3 + \dots.$$

Wegen der Linearität der formalen Ableitung muss man das nur für Monome $f(X) = X^n$ zeigen:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}h^k = \sum_{k=0}^{n} \frac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{k!}x^{n-k}h^k = \sum_{k=0}^{n}\frac{1}{k!}\partial^k(x^n)h^k.$$

Theorem 7. *(Hensel'sches Lemma) Sei* $f(X) \in \mathbb{Z}_p[X]$ *und* $\alpha_1 \in \mathbb{Z}_p$, *sodass* $f(\alpha_1) = 0 \mod p$ *sowie* $f'(\alpha_1) \neq 0 \mod p$. *Dann existiert ein* $\alpha \in \mathbb{Z}_p$, *sodass* $f(\alpha) = 0$.

Proof. Wir konstruieren eine Folge $\alpha_n \in \mathbb{Z}_p$, sodass

$$i)\ f(\alpha_n) \equiv 0 \mod p^n, \qquad ii)\ \alpha_{n+1} \equiv \alpha_n \mod p.$$

D.h. (α_n) ist eine Cauchy-Folge mit Grenzwert $\alpha \in \mathbb{Z}_p$, und es gilt $f(\alpha) = \lim_{n\to\infty} f(\alpha_n) = 0$, da dies mod p^n für alle n gilt.

α_1 existiert nach Voraussetzung. Es muss $\alpha_2 = \alpha_1 + b_1 p$ gelten. Damit:

$$f(\alpha_2) = f(\alpha_1 + b_1 p) = f(\alpha_1) + f'(\alpha_1) b_1 p + p^2 \cdot \text{Rest}$$

nach der Taylorentwicklung. D.h. es muss $0 \equiv f(\alpha_1) + f'(\alpha_1) b_1 p \mod p^2$ gelten. Nun hat man $f(\alpha_1) = x_1 p$ nach der Voraussetzung und $f'(\alpha_1)$ ist invertierbar $\mod p$, sodass $b_1 = -x_1 \cdot f'(\alpha_1)$ eindeutig bestimmt ist und existiert. Allgemeiner kann man so die α_n konstruieren. □

Proof. (Theorem 3) Die schwierige Richtung ist zu zeigen, dass wir eine Lösung in $\mathbb{Q}$ haben, wenn wir eine Lösung für alle $\mathbb{Q}_p$ annehmen. Wir nehmen an, dass a, b quadratfrei und in $\mathbb{Z}$ sind und führen Induktion nach $\max(|a|, |b|)$. Falls $a = 1$ oder $b = 1$, so hat man eine Lösung in $\mathbb{Q}$. Falls $\max(|a|, |b|) = 1$, so gilt $a > 0$ oder $b > 0$, da $(a, b)_\infty = 1$, d.h. $a = 1$ oder $b = 1$, sodass wir eine Lösung in $\mathbb{Q}$ haben. Sei also $\max(|a|, |b|) > 1$, und o.E. $|a| \leq |b|$. Sei $|b| = \prod_i p_i^{n_i}$ die Primfaktorzerlegung von $|b|$, sodass $n_i = 0, 1$, da b quadratfrei ist. Dann ist $a \mod b$ ein Quadrat in $\mathbb{Z}/b\mathbb{Z} \cong \bigoplus \mathbb{Z}/p_i\mathbb{Z}$. Sonst wäre $a \mod p$ für eines der $p = p_i$ kein Quadrat. Dann gilt $p \neq 2$ (sonst wäre es wieder ein Quadrat), d.h. $(a, b)_p = \left(\frac{a}{p}\right) = -1$ (hier benutzen wir 1. und 2. von Proposition 6 sowie 4. von Satz 4), im Widerspruch zu $(a, b)_p = 1$.

Damit existiert ein $r \in \mathbb{Z}$, sodass $r^2 \equiv a \mod b$, und wir können $0 \leq r \leq |b|/2$ wählen, da jedes Element $\mathbb{Z}/b\mathbb{Z}$ einen Repräsentanten $-|b|/2 \leq n \leq |b|/2$ hat.

Sei $r^2 - c = bc$, $c \in \mathbb{Z}$. Falls $c = 0$, so $a = r^2$, sodass $a(1/r)^2 + b \cdot 0^2 = 1$ eine Lösung in $\mathbb{Q}$ hat. Sei also $c \neq 0$. Dann gilt

$$|c| = \left|\frac{r^2 - a}{b}\right| \leq \left|\frac{r^2}{b}\right| + \left|\frac{a}{b}\right| \leq \frac{|b|}{4} + 1 < |b|,$$

da $|b| > 2$. Ist nun $|a| < |b|$, so existiert nach Induktionsvoraussetzung und Lemma 8 ein Lösung in $aX^2 + cY^2 = Z^2$ wegen $|c| < |b|$, was eine Lösung für a, b impliziert. Ist $|a| = |b|$, so erhält man eine Lösung, indem man auf den Fall $|a| < |b|$ reduziert, indem man a durch c ersetzt.

□

Lemma 8. *Sei K ein Körper, $a, b, c \in K^\times$, $r \in K$ und $r^2 - a = bc$. Dann hat man eine Bijektion zwischen den nicht-trivialen Lösungen von $aX^2 + bX^2 = Z^2$ und $aX^2 + cX^2 = Z^2$, gegeben durch $f(x, y, z) = (rx + z, by, ax + rz)$ bzw. $g(x, y, z) = (rz - z, cy, -ax + rz)$.*