Zahlentheorie

Leonhard Summerer

LaTeX-Satz: Anton Mosich

Wintersemester 2023

Inhaltsverzeichnis

1 Binäre quadratische Formen

1.1 Summe von 2 Quadraten

$$n = x^2 + y^2 \quad n \in \mathbb{N}, x, y \in \mathbb{Z}$$

Proposition 1.1.1:
Sind $m, n \in \mathbb{N}$ Summe von zwei Quadraten, so ist es auch $m \cdot n$.

Beweis. Sei $m = a^2 + b^2, n = x^2 + y^2$.

$$mn = (a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2$$
$$(= (ax - by)^2 + (ay + bx)^2)$$

□

$\longrightarrow$ Es genügt, den Fall $n = p \in \mathbb{P}$ zu untersuchen.

Satz 1.1.2:

1. $2 = 1 + 1$
2. $p \equiv 3 \pmod 4$ ist niemals Summe von zwei Quadraten
3. $p \equiv 1 \pmod 4$ ist eindeutig als Summe von zwei Quadraten darstellbar

Beweis.

1. klar
2. $\square \equiv 0, 1 \pmod 4 \implies \square + \square \equiv 0, 1, 2 \pmod 4$
3. Sei $p \equiv 1 \pmod 4$

   Existenz: $x^2 \equiv -1 \pmod p$ ist lösbar, das heißt $p \mid x^2 + 1, \exists k\colon pk = x^2 + 1$. Wähle k minimal, sodass $pk = x^2 + y^2$ mit $(x, y) = 1$. Wähle $a, b\colon x \equiv a \pmod p, y \equiv b \pmod p$ mit $|a|, |b| \leq \frac{p}{2}$. Dann ist $a^2 + b^2 \equiv 0 \pmod p$ und $a^2 + b^2 \leq \frac{p^2}{2}$. Es folgt: das minimale k erfüllt $1 \leq k \leq \frac{p}{2}$. Behauptung: es gilt $k = 1$. Angenommen $k > 1$. Seien $x \equiv u \pmod k, y \equiv v \pmod k$ mit $|u|, |v| \leq \frac{k}{2}$. Es ist $u^2 + v^2 \equiv 0 \pmod k$, also $u^2 + v^2 = k \cdot l$ mit $1 \leq l \leq \frac{k}{2} < k$.

   $$(pk)(kl) = pk^2 l = (x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2$$

Es ist $xu + yv \equiv x^2 + y^2 \equiv 0 \pmod{k}$, $xv - yu \equiv 0 \pmod{k}$. Also $xu + yv = kx_0$, $xv - yu = ky_0$. Es folgt: $pl = x_0^2 + y_0^2$ mit $l < k$ ein Widerspruch zur Voraussetzung $k > 1$.

Eindeutigkeit: Angenommen $p = c^2 + d^2 = a^2 + b^2$ mit $a \equiv c \pmod{2}$ und $b \equiv d \pmod{2}$.

$$\begin{aligned} a^2 + b^2 = c^2 + d^2 &\iff a^2 - c^2 = d^2 - b^2 \\ &\iff \frac{a-c}{2}\frac{a+c}{2} = \frac{d-b}{2}\frac{d+b}{2} \quad (a \neq c, b \neq d) \end{aligned}$$

Sei $s := \mathrm{ggT}(\frac{a-c}{2}, \frac{d-b}{2})$. Dann ist $\frac{a-c}{2} = st$, $\frac{d-b}{2} = su$ und es gilt $t \cdot \frac{a+c}{2} = u \cdot \frac{d+b}{2}$. Es ist $(u,t) = 1$. $\frac{a+c}{2} = u \cdot v$ und $\frac{d+b}{2} = t \cdot v$.

$$\begin{aligned} a &= st + uv \\ b &= tv - su \\ p = a^2 + b^2 &= (st + uv)^2 + (tv - su)^2 = \underbrace{(u^2 + t^2)}_{\geq 2}\underbrace{(s^2 + v^2)}_{\geq 2} \quad (1.1.1) \end{aligned}$$

□

Korollar 1.1.3:
$n = \square + \square \iff n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ mit $\alpha_i \equiv 0 \pmod{2}$ falls $p_i \equiv 3 \pmod{4}$.

Beweis. $\Longrightarrow$: Sei $p \equiv 3 \pmod{4}$ mit $p \mid n$ und $n = x^2 + y^2$, sodass $x^2 + y^2 \equiv 0 \pmod{p}$.

$$x^2 \equiv (-1) \cdot y^2 \pmod{p} \implies x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \cdot y^{p-1} \pmod{p}.$$

Falls $p \nmid x (\implies p \nmid y)$, so folgte $1 \equiv -1 \pmod{p}$, ein Widerspruch. Also gilt $p \mid x \wedge p \mid y$, daher $p^2 \mid x^2 + y^2$.

$\Longleftarrow$: Schreibe $n = m^2 \cdot n'$, wobei alle Primfaktoren von n' kongruent 1 mod 4 sind. Nach Theorem 1.1.1 ist $n' = x^2 + y^2$, somit $m^2 n' = (mx)^2 + (my)^2$. □

Aufgaben:

1. Bestimme alle $n \in \mathbb{N}$: $n = \square - \square$.
2. Bestimme alle $n \in \mathbb{N}$: $n = \square_{>0} + \square_{>0}$.
3. Zeige dass $n \neq \underbrace{\square}_{\in\mathbb{Z}} + \underbrace{\square}_{\in\mathbb{Z}} \implies n \neq \underbrace{\square}_{\in\mathbb{Q}} + \underbrace{\square}_{\in\mathbb{Q}}$.

1.2 Binäre quadratische Formen (BQF)

Definition 1.2.1:
Eine Funktion

$$f: \quad \mathbb{Z}^2 \to \mathbb{Z}$$
$$(x, y) \mapsto ax^2 + bxy + cy^2$$

heißt BQF.
f stellt m dar $:\iff \exists (x, y): m = ax^2 + bxy + cy^2$

Es gilt $a = f(1,0), c = f(0,1), b = f(1,1) - f(1,0) - f(0,1)$. Schreibe $f = (a, b, c)$.

Definition 1.2.2:
Zwei Formen f, g heißen äquivalent ($f \sim g$) falls $\exists U \in \mathrm{SL}_2(\mathbb{Z})$ mit $f \circ U = g$. Ist $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, so stellen f und $f \circ U$ dieselben Zahlen dar.

$$f(x, y) = m \iff f \circ U \left(U^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \right) = m$$

$$f \circ E = f, f \circ U = g \implies f = g \circ U^{-1}, f \circ U = g, g \circ V = h \implies f \circ UV = h.$$

Definition 1.2.3:
Für $f = (a, b, c)$ schreiben wir

$$D(f) := -\begin{vmatrix} 2a & b \\ b & 2c \end{vmatrix} = b^2 - 4ac$$

für die Diskriminante von f.

Proposition 1.2.4:
Sei $f = (a, b, c)$ und $f \circ U = (A, B, C)$ mit $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2 \mathbb{Z}$. Dann gilt:

1. $A = a\alpha^2 + b\alpha\gamma + c\gamma^2$,
   $B = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta$,
   $C = a + \beta^2 + b\beta\delta + c\delta^2$

2. $\begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix} = U^t \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} U$

3. $D(f) = D(f \circ U)$

Beweis. 1.

$$A = (f \circ U)(1,0) = f\left(U \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = f(\alpha, \gamma)$$

$$C = (f \circ U)(0,1) = f\left(U \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = f(\beta, \delta)$$

$$B = f\left(U \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) - f\left(U \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) - f\left(U \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = f(\alpha + \beta, \gamma + \delta) - f(\alpha, \gamma) - f(\beta, \delta)$$

2.

$$f(x,y) = \begin{pmatrix} x \\ y \end{pmatrix}^t \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

$$\implies (f \circ U)(x,y) = f\left(U \begin{pmatrix} x \\ y \end{pmatrix}\right) = \left(U \begin{pmatrix} x \\ y \end{pmatrix}\right)^t \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} U \begin{pmatrix} x \\ y \end{pmatrix}$$

$$= \begin{pmatrix} x \\ y \end{pmatrix}^t \left[U^t \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} U \right] \begin{pmatrix} x \\ y \end{pmatrix} = (A, B, C)$$

3. folgt unmittelbar aus Punkt 2. □

Für $D(f)$ mit $f = (a,b,c)$ gilt $D \equiv 0,1 \pmod 4$, denn $D(f) = b^2 - 4ac \equiv b^2 \pmod 4$. Für festes $D \equiv 0 \pmod 4$ ist $f = (1, 0, \frac{-D}{4})$ die Hauptform zur Diskriminante D. Für festes $D \equiv 1 \pmod 4$ ist $f = (1, 1, \frac{1-D}{4})$ die Hauptform zur Diskriminante D.

Definition 1.2.5:

Eine BQF f heißt positiv (negativ) definit, falls $f(x,y) > 0 \quad (f(x,y) < 0)$ für alle $(x,y) \neq (0,0)$. f heißt indefinit, falls $\exists (x_1,y_1),(x_2,y_2) : f(x_1,y_1) > 0 \wedge f(x_2,y_2) < 0$

Bemerkung 1.2.6:

Falls $D(f) = 0$, so existieren f, die weder positiv definit, negativ definit noch indefinit sind. $f = (a,b,c) \implies$

$$4af(x,y) = (2ax + by)^2 - D(f)y^2. \tag{1.1}$$

f hat für $D(f) = 0$ konstantes Vorzeichen, aber $\exists (x,y) \neq (0,0)$ mit $f(x,y) = 0$.

$\begin{cases} a \neq 0 : (x,y) = (-b, 2a) \\ a = 0 : (x,y) = (1,0) \end{cases}$

Satz 1.2.7:
f sei eine BQF.

1. f ist positiv (negativ) definit $\iff D(f) < 0 \wedge a > 0\ (a < 0)$
2. f ist indefinit $\iff D(f) > 0$

Beweis. 1. Sei $D(f) < 0 \wedge a > 0$. Aus Gleichung (1.1) folgt $f(x,y) > 0 \forall (x,y) : (x,y) \neq (0,0)$.
Umgekehrt wissen wir dass $D(f) \neq 0$. Wäre $D(f) > 0$, so folgte aus Gleichung (1.1) die Existenz negativer Werte ($4af(-2a,b) = -Db^2$).

2. Sei $D(f) > 0$. $4af(-2a,b) < 0 \wedge 4af(1,0) > 0$ falls $a \neq 0$. Falls $a = 0$ ist $f(x,1) = bx + c$.
Umgekehrt wissen wir aus Punkt 1, dass $D(f) \geq 0$ gelten muss. Wäre $D(f) = 0$, so folgte aus Gleichung (1.1), dass das Vorzeichen von f konstant ist, falls $a \neq 0$. Falls $a = 0$, so ist $b = 0$, also $f = cy^2$. □

1.3 Positiv definite binäre quadratische Formen (PDBQF)

f NDBQF $\implies -f$ PDBQF.

$\mathrm{SL}_2(\mathbb{Z}) = \langle S, T \rangle$, wobei $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

$$S^g = \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix}, T^2 = -E$$

Direktes Nachrechnen liefert für $f = (a,b,c)$:

$$f \circ S^g = (a, 2ag + b, ag^2 + bg + c), \quad f \circ T = (c, -b, a)$$

Bemerkung 1.3.1:
$\sim$ ist Äquivalenzrelation auf der Menge der PDBQF. $\longrightarrow$ es genügt in jeder Äquivalenzklasse eine form zu untersuchen.

Definition 1.3.2:
$f = (a,b,c)$ PDBQF heißt reduziert, wenn

$$|b| \leq a \leq c.$$

Wir zeigen: jede Äquivalenzklasse enthält mindestens eine reduzierte Form.

Lemma 1.3.3:
Ist $f = (a, b, c)$, so existiert ein $\alpha \in \{0, 1\}$ und ein $g \in \mathbb{Z}$ mit

$$f \circ T^\alpha S^g = (a_1, b_1, c_1) \text{ mit } |b_1| \leq a_1 = \min\{a, c\}$$

Beweis. Falls $a \leq c$ wähle $\alpha = 0$. Falls $a > c$, wähle $\alpha = 1$. Mit $f \circ T^\alpha = (a', b', c') =: f'$ gilt: $a' = \min\{a, c\}$ und $|b'| = |b|$. Wähle nun g so, dass $\left|g + \frac{b'}{2a'}\right| \leq \frac{1}{2} \iff |2a'g + b'| \leq a'$. Dann ist $f' \circ S^g = (a', b' + 2a'g, a'g^2 + b'g + c')$ und somit

$$a_1 = a', |b_1| = |b' + 2a'g| \leq a' = a_1 = \min\{a, c\}.$$ □

Satz 1.3.4:
Jede PDBQF ist zu einer reduzierten Form $f \circ U$ äquivalent. Dabei ist $U = T^\alpha S^{g_1} T S^{g_2} T \cdots T S^{g_k}$ mit $\alpha \in \{0, 1\}, g_i \in \mathbb{Z}, k \in \mathbb{N}$.

Beweis. Wähle gemäß Theorem 1.3.3 α_1, g_1 so, dass $f \circ T^{\alpha_1} S^{g_1} = (a_1, b_1, c_1)$ mit $|b_1| \leq a_1 = \min\{a, c\}$. Seien $\alpha_j \in \{0, 1\}$ und $g_j \in \mathbb{Z}$ bereits gewählt für $1 \leq j \leq n - 1$. Dann seien α_n, g_n so gewählt, dass $f \circ T^{\alpha_1} S^{g_1} \cdots T^{\alpha_n} S^{g_n} = (a_n, b_n, c_n)$ mit $|b_n| \leq a_n = \min\{a_{n-1}, c_{n-1}\}$. Dann ist $1 \leq a_n \leq a_{n-1}$ und es existiert ein k mit $a_k = a_{k+1}$. Es ist $|b_k| \leq a_k$. Wäre $c_k < a_k$, so wäre $a_k = a_{k+1} = \min\{a_k, c_k\} = c_k < a_k$, ein Widerspruch. Also ist (a_k, b_k, c_k) reduziert. □

Beispiel 1.3.5:

$$f = (5, -4, 2), D(f) = -26$$
$$f \sim (2, 4, 5) \quad g = -1 \text{ wegen } \frac{-4}{2 \cdot 2} = -1$$
$$(2, 4, 5) \circ S^g = (2, 4 + 4g, 2g^2 + 4g + 5)$$
$$\text{mit } g = -1 : f \sim (2, 0, 3) \text{ ist reduziert.}$$

Proposition 1.3.6:
Sei $f = (a, b, c)$ PDBQF und reduziert.

1. $a = \min\{f(x,y) \colon x \neq 0\}$.
2. $c = \min\{f(x,y) \colon y \neq 0\}$.
3. $a - |b| + c = \min\{f(x,y) \colon x \neq 0, y \neq 0\}$.
4. $f(x,y) = a$ hat die Lösungen
   a) $(1,0), (-1,0)$ für $|b| \leq a < c$,
   b) $(1,0), (-1,0), (0,1), (0,-1)$ für $|b| < a = c$,
   c) $(1,0), (-1,0), (0,1), (0,-1), (1,-\operatorname{sgn}(b)), (-1,\operatorname{sgn}(b))$ für $|b| = a = c$.
5. $f(x,y) = a - |b| + c$ hat die Lösungen ($x \neq 0, y \neq 0$):

$$\begin{cases} (1,-\operatorname{sgn}(b)), (-1,\operatorname{sgn}(b)) & \text{falls } b \neq 0 \\ (1,1), (1,-1), (-1,1), (-1,-1) & \text{falls } b = 0 \end{cases}$$

Beweis. Behauptung: $|x| > |y| \implies f(x,y) > (a - |b| + c) \cdot y^2$.

$$\begin{aligned} f(x,y) &= ax^2 + bxy + cy^2 \geq ax^2 - |b|\,xy + cy^2 \\ &> axy - |b|\,xy + cy^2 = (a - |b|)xy + cy^2 \\ &\geq (a - |b| + c)y^2 \end{aligned}$$

Analog, falls $|y| > |x| \implies f(x,y) > (a - |b| + c)x^2$.

Für $|xy| > 1$ gilt: $f(x,y) > a - |b| + c \underbrace{\geq c \geq a}_{\text{da } f \text{ reduziert}}$.

Für $|xy| \leq 1$: falls $x \neq 0, y \neq 0$ folgt $|x| = |y| = 1$ und $f(x,y) \geq a - |b|\,|xy| + c = a - |b| + c$. Durch Einsetzen erhalten wir Punkte 3 und 5.

Falls $f(x,y) = a$ und $a - |b| + c > a$ folgt $x = 0$ oder $y = 0$. Falls $y = 0$, folgt $|x| = 1$, woraus Punkte 1 und 4a folgen.

Falls $|y| = 1$ und $x = 0$, so ist $a = f(x,y) = c$ und $f(0,1) = f(0,-1) = a$, also Punkt 4b.

Falls $a - |b| + c = a$, das heißt $|b| = c = a$, und $|xy| = 1$, so ist $f(x,y) \geq a - |b|\,|xy| + c = a - |b| + c = a$ und Punkt 4c folgt.

Für $|x| = |y| = 1$ ist $f(x,y) \geq a - |b| + c \geq c$. $f(0,1) = f(0,-1) = c$ liefert Punkt 2. □

Definition 1.3.7:

$a - |b| + c \geq c \geq a$ heißen drittes / zweites / erstes Minimum von $f = (a,b,c)$.

Satz 1.3.8:
In jeder Äquivalenzklasse PDBQF liegen höchstens 2 reduzierte Formen. In diesem Fall gilt:

$$f = (a, b, a) \sim (a, -b, a) \text{ oder } f = (a, \pm a, c) \sim (a, \mp a, c)$$

Beweis. Seien (a, b, c) und (a', b', c') beide reduziert: $|b| \leq a \leq c, |b'| \leq a' \leq c'$. Falls $(a, b, c) \sim (a', b', c')$, so stellen sie dieselben Zahlen mit derselben Anzahl von Lösungen dar. Insbesondere: $a = \min\{f(x, y) \colon x \neq 0\} = \min\{f'(x, y) \colon x \neq 0\} = a'$. Wenn $c > a$, so ist c die nächstgrößte von f beziehungsweise f' dargestellte Zahl. $f(x, y) = a$ hat genau 2 Lösungen $\implies$ $f'(x, y) = a$ hat auch genau 2 Lösungen $\implies$ $c' > a'$ $\implies$ c' ist die nächstgrößte von f' dargestellte Zahl. Insgesamt also $c = c'$.

Wegen $D(f) = D(f')$ ist $|b| = |b'|$. Lediglich $(a, b, c) \sim (a, -b, c)$ ist möglich.

Sei $(a, b, c) \circ U = (a, -b, c) \implies U = \pm \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} = \pm S^{\beta}$. Durch Einsetzen folgt $-b = 2a\beta + b$, woraus folgt dass $a \mid b$. Wegen $|b| \leq a$ folgt $|b| = a$.

Falls $c = a$, so ist $U = T$. □

Satz 1.3.9:
Sei $D < 0$. Dann gibt es höchstens endlich viele Äquivalenzklassen PDBQF mit $D(f) = D$.

Beweis. Es genügt zu zeigen, dass es höchstens endlich viele reduzierte Formen mit $D(f) = D$ gibt.

$$\begin{aligned} f(a, b, c) \text{ reduziert} &\implies |b| \leq a \leq c \implies b^2 \leq ac \\ &\implies |D(f)| = 4ac - b^2 \geq 3ac \geq 3a^2 \\ &\implies 1 \leq a \leq \sqrt{\frac{|D|}{3}},\ 0 \leq |b| \leq a \leq \sqrt{\frac{|D|}{3}} \\ (\ &\implies \text{nur endlich viele Möglichkeiten für } a, b) \end{aligned}$$

$D = b^2 - 4ac$ bestimmt c eindeutig, wenn a, b gegeben sind. □

Definition 1.3.10:
Die Anzahl der Äquivalenzklassen PDBQF mit $D(f) = D$ heißt Klassenzahl $h(D)$.

Beispiel 1.3.11:

1. $D = -3 \implies a \leq \sqrt{\frac{|D|}{3}} \implies a = 1, b^2 - 4c = -3$. $b = 0$ nicht möglich (wegen mod 4) $\implies |b| = 1 \implies c = 1$. 2 reduzierte Formen mit $D(f) = -3$: $(1,1,1), (1,-1,1)$. Diese sind äquivalent $\implies h(-3) = 1$.
2. $D = -4 \implies 1 \leq a \leq \sqrt{\frac{4}{3}} \implies a = 1 \implies b^2 - 4c = -4 \overset{\text{mod } 4}{\implies} b = 0 \implies c = 1 \implies (1,0,1)$ einzige reduzierte Form, $h(-4) = 1$.
3. $D = -15 \implies 1 \leq a \leq \sqrt{5} \implies a \in \{1,2\}$
   1. Fall $a = 1 \implies b^2 - 4c = -15 \implies |b| \in \{0,1\} \overset{\text{mod } 4}{\implies} |b| = 1 \implies c = 4 \implies (1,1,4), (1,-1,4)$ sind äquivalent
   2. Fall $a = 2 \implies b^2 - 8c = -15 \implies |b| \in \{0,1,2\} \overset{\text{mod } 4}{\implies} |b| = 1 \implies c = 2 \implies (2,1,1), (2,-1,2) \implies h(-15) = 2$

Definition 1.3.12:

f sei PDBQF und $U \in \mathrm{SL}_2(\mathbb{Z})$, dann heißt U ein Automorphismus von f, falls $f \circ U = f$. Schreibe $U \in A(f)$.

Proposition 1.3.13:

f PDBQF, $U \in \mathrm{SL}_2(\mathbb{Z})$. Dann ist $A(f) \leq SL_2(\mathbb{Z})$ und weiters ist $A(f)$ zu $A(f \circ U)$ konjugiert.

Beweis. Übung □

Satz 1.3.14:

Sei $f = (a,b,c)$ reduziert.

1. Falls $a < c$ oder $c > |b| > 0$, so ist $A(f) = \{E, -E\}$ (allgemeiner Fall).
2. Falls $a = c > |b| = 0$, so ist $A(f) = \{E, T, T^2, T^3\} = \langle T \rangle$.
3. Falls $a = c = |b|$, so ist $A(f) = \langle R \rangle$ mit $R = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, wobei R Ordnung 6 hat.

Definition 1.3.15:

Sei $m \in \mathbb{Z}, f$ PDBQF, $x_0, y_0 \in \mathbb{Z}$ mit $f(x_0, y_0) = m$. Diese Darstellung von m heißt eigentlich, falls $\mathrm{ggT}(x_0, y_0) = 1$, ansonsten uneigentlich.

Beispiel 1.3.16:

$$f(x,y) = x^2 - y^2 \quad m = 48$$
$$48 = \underbrace{8^2 - 4^2}_{\text{uneigentlich}} = \underbrace{7^2 - 1^2}_{\text{eigentlich}}$$

Bemerkung 1.3.17:

Ist $m \in \mathbb{Z}$ quadratfrei, so ist jede Darstellung von m eigentlich.

Wir schränken uns nun auf die Untersuchung eigentlicher Darstellungen ein.
Sei $f(\alpha, \gamma) = m$ eine eigentliche Darstellung von m durch f.

$$\mathrm{ggT}(\alpha, \gamma) = 1 \implies \exists \beta_0, \delta_0 \in \mathbb{Z} \colon \alpha\delta_0 - \beta_0\gamma = 1$$

Wir setzen $U_t := \begin{pmatrix} \alpha & \beta_0 + t\alpha \\ \gamma & \delta_0 + t\gamma \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. $f \circ U_t \begin{pmatrix} 1 \\ 0 \end{pmatrix} = f(\alpha, \gamma) = m$

$f \circ U_t = (A_t, B_t, C_t)$ mit $A_t = m, B_t = 2a\alpha\beta_0 + b(\alpha\delta_0 + \gamma\beta_0) + 2c\gamma\delta_0 + 2tm$. Wähle jetzt $t = t_0$ so, dass $0 \le B_{t_0} < 2m$, B_{t_0} ist unabhängig von β_0, δ_0 und heißt Minimalwurzel der Darstellung $f(\alpha, \gamma) = m$. Mit $U_t = U_{t_0}$ gilt $f \circ U_{t_0} = (m, B_{t_0}, C_{t_0})$ mit $0 \le B_{t_0} < 2m$.

Aus $D(f) = D(f \circ U_{t_0})$ folgt

$$B_{t_0}^2 - 4mC_{t_0} = D(f) \tag{1.2}$$
$$\implies C_{t_0} = \frac{1}{4m} \cdot (B_{t_0}^2 - D(f))$$

Aus Gleichung (1.2) folgt $z^2 \equiv D(f) \pmod{4m}$ ist lösbar, $(z = B_{t_0})$ mit einer Lösung $0 \le z \le 2m$.

Satz 1.3.18:

Sei f PDBQF, $m > 0$ quadratfrei. Seien $\{B_1, \ldots, B_k\}$ die Lösungen von $B^2 \equiv D(f) \pmod{4m}$ mit $0 \le B_i \le 2m$ für $i = 1, \ldots, k$. Setze $C_i := \frac{1}{4m}(B_i^2 - D(f))$ und $f_i = (m, B_i, C_i)$. Für

$1 \le i \le t \le k$ gelte zudem $f_i \sim f$, das heißt $\exists U_i = \begin{pmatrix} \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ mit $f_i = f \circ U_i$. Dann gilt: $\left\{ VU_i \begin{pmatrix} 1 \\ 0 \end{pmatrix} : V \in A(f), 1 \le i \le t \right\}$ ist Lösungsmenge von $f(x,y) = m$. Die Anzahl der Lösungen ist genau $t \cdot |A(f)|$.

Beweis. Sei $V \in A(f)$ und $1 \le i \le t$ fest. $m = f_i(1,2) = f \circ U_i(1,0) = f \circ VU_i(1,0)$, das heißt VU_i ist Lösung.

Umgekehrt: Sei $f(x,y) = m$ und U_{t_0} die zu dieser Darstellung gehörende Matrix. Dann ist $U_{t_0} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$ und $f \circ U_{t_0} = (m, B, C)$ mit $B^2 \equiv D(f) \pmod{4m}$, mit $0 \le B < 2m, C = \frac{1}{4m}(B^2 - D(f))$. Es folgt: $\exists 1 \le i \le k$ mit $B = B_i, C = C_i$ und daher $f \circ U_{t_0} = f_i$, sodass sogar $1 \le i \le t$ gelten muss.

Daher gilt: $f_i = f \circ U_{t_0} = f \circ U_i \implies f = f \circ \underbrace{U_{t_0} \circ U_i^{-i}}_{=:V} \implies U_{t_0} \circ U_i^{-1} \in A(f)$. Also $U_{t_0} = VU_i$ und $\begin{pmatrix} x \\ y \end{pmatrix} = VU_i \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Es verbleibt zu zeigen: $VU_i \begin{pmatrix} 1 \\ 0 \end{pmatrix} = U_j \begin{pmatrix} 1 \\ 0 \end{pmatrix} \implies V = E$ und $i = j$.

Sei dazu $V = \begin{pmatrix} v_1 & v_2 \\ v_3 & v_4 \end{pmatrix}$. $V \begin{pmatrix} \alpha_i \\ \gamma_i \end{pmatrix} = \begin{pmatrix} \alpha_j \\ \gamma_j \end{pmatrix}, \alpha_i\delta_i - \beta_i\gamma_i = 1, \alpha_j\delta_j - \beta_j\gamma_j = 1 (U_i, U_j \in \mathrm{SL}_2(\mathbb{Z}))$ Aus $\begin{pmatrix} \alpha_i \\ \gamma_i \end{pmatrix} = V^{-1} \begin{pmatrix} \alpha_j \\ \gamma_j \end{pmatrix} = \begin{pmatrix} v_4 & -v_2 \\ -v_3 & v_1 \end{pmatrix} \begin{pmatrix} \alpha_j \\ \gamma_j \end{pmatrix}$ folgt $\alpha_i = v_4\alpha_j - v_2\gamma_j, \gamma_i = -v_3\alpha_j + v_1\gamma_j$.

$$1 = (v_4\alpha_j - v_2\gamma_j)\delta_i - \beta_i(-v_3\alpha_j + v_1\gamma_j) \iff \alpha_j(v_4\delta_i + v_3\beta_i) - \gamma_j(v_2\delta_i + v_1\beta_i) = 1$$

$$\implies \exists g \in \mathbb{Z}: \begin{cases} \delta_j = v_4\delta_i + v_3\beta_i + g\delta_j \\ \beta_j = v_2\delta_i + v_1\beta_i + g\alpha_j \end{cases}$$

Das heißt $\begin{pmatrix} \beta_j \\ \delta_j \end{pmatrix} = V \begin{pmatrix} \beta_i \\ \delta_i \end{pmatrix} + g \begin{pmatrix} \alpha_j \\ \gamma_j \end{pmatrix} = V \begin{pmatrix} \beta_i + g\alpha_i \\ \delta_i + g\gamma_i \end{pmatrix}$. Das heißt $U_j = VU_iS^g$ für $g \in \mathbb{Z}$. Also ist $f \circ U_j = f \circ U_iS^g$ und wegen $0 \le B_i, B_j < 2m$ ist $g = 0$ und daher $f_j = f \circ U_j = f \circ U_i = f_i$, sodass $B_i = B_j, i = j, V = E$. □

Beispiel 1.3.19:

Finde alle Lösungen von $121x^2 + 98xy + 20y^2 = 17$. $f = (121, 98, 20), D(f) = -76$.

$f \sim (20, -98, 121)$. Bestimme g: nächste ganze Zahl an $\frac{98}{2 \cdot 20} \implies g = 2, f \circ S^g = (20, -18, 20 \cdot 4 - 98 \cdot 2 + 121) = (20, -18, 5)$.

$(20, -18, 5) \sim (5, 18, 20)$. Bestimme g: nächste ganze Zahl an $\frac{-18}{10} \implies g = -2, f \circ S^{-2} = (5, -2, 4)$ ist reduziert.

$$(4, 2, 5) = f \circ \underbrace{TS^2TS^{-2}T}_{U}, \text{ mit } U = \begin{pmatrix} -2 & -1 \\ 5 & 2 \end{pmatrix}$$

Bestimme alle Lösungen von $4x^2 + 2xy + 5y^2 = 17$.

Bestimme alle Lösungen < 34 von $B^2 \equiv -76 \pmod{4 \cdot 17}$. Das sind genau die Lösungen von $Z^2 \equiv -2 \pmod{17}$. Lösungen sind 7 und 10. Mit $B = 2Z$ ergibt sich $B = 14, B = 20$ für die Minimalwurzeln. Die zugehörigen Formen sind $(17, 14, \frac{1}{4 \cdot 17}(14^2 + 76)) = (17, 14, 4)$ und $(17, 20, 7)$. Überprüfe, welche der Formen zu $(4, 2, 5)$ äquivalent ist.

$$f_1 = (17, 14, 4) \sim (4, -14, 17) \sim (4, 2, 5)$$
$$f_2 = (17, 20, 7) \sim (7, -20, 17) \sim (7, -6, 4) \sim (4, 6, 7) \sim (4, -2, 5) \nsim (4, 2, 5)$$
$$f_1 \circ TS^2 = (4, 2, 5) = f \circ U \implies f_1 = f \circ U \circ S^{-}2T^{-1}$$
$$U = \begin{pmatrix} -2 & -1 \\ 5 & 2 \end{pmatrix}, S^{-2}T = \begin{pmatrix} -2 & -1 \\ 1 & 0 \end{pmatrix} (T^{-1} = -T)$$
$$\begin{pmatrix} -2 & -1 \\ 5 & 2 \end{pmatrix} \cdot \begin{pmatrix} -2 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ -8 & -5 \end{pmatrix}$$
$$\begin{pmatrix} 3 & 2 \\ -8 & -5 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ -8 \end{pmatrix}$$
$$\begin{pmatrix} -3 & -2 \\ 8 & 5 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -3 \\ 8 \end{pmatrix}$$

sind Lösungen der ursprünglichen Gleichung.

Beispiel 1.3.20:

$x^2 + y^2 = m, f = (1, 0, 1), D(f) = -4, f$ reduziert, $h(-4) = 1$.

Satz 1.3.21:

Sei $m = 2^\alpha p_1 \cdots p_k$ quadratfrei. Falls $\exists i \colon 1 \le i \le k$ mit $p_i \equiv 3 \pmod{4}$, so hat $x^2 + y^2 = m$ keine Lösung. Falls $p_i \equiv 1 \pmod{4}$, $1 \le i \le k$, so hat $x^2 + y^2 = m$ genau 2^{k+2} Lösungen (in $\mathbb{Z}$).

Beweis. $f = (1, 0, 1)$. $B^2 \equiv -4 \pmod{4m}$. Falls $\exists i \colon 1 \le i \le k$ mit $p_i \equiv 3 \pmod{4}$, so hat $z^2 \equiv -1 \pmod{p_i}$ keine Lösung, daher auch $z^2 \equiv -1 \pmod{m}$ keine.

Falls $p_i \equiv 1 \pmod{4}$, $1 \le i \le k$, die Lösungen von $B^2 \equiv -4 \pmod{4m}$, die kleiner $2m$ sind, entsprechen genau den Lösungen von $z^2 \equiv -1 \pmod{m}$. Für jedes i hat $\begin{matrix} z^2 \equiv -1 \pmod{p_i} \\ z^2 \equiv -1 \pmod{2^\alpha} \end{matrix}$ genau $\begin{matrix} 2 \\ 1 \end{matrix}$ Lösungen. Daher hat $z^2 \equiv -1 \pmod{m}$ nach dem CRS genau 2^k Lösungen. Wegen $|A(f)| = 4$ für $f = (1, 0, 1)$ gibt es 2^{k+2} Lösungen. □

Aufgaben:

1. Bestimme die zu $f = (133, 108, 22)$ äquivalente, reduzierte Form.
2. Bestimme $h(-20)$.
3. Zeige: $\mathbb{P} \ni p = x^2 + 5y^2 \iff p \equiv 1, 9 \pmod{20}$

1.4 Summen von 4 Quadraten

Satz 1.4.1 (Lagrange):
Jedes $n \in \mathbb{N}$ ist Summe von 4 Quadraten ganzer Zahlen. ($n = x^2 + y^2 + z^2 + w^2$ mit $x, y, z, w \in \mathbb{Z}$)

Beweis.

$$(x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) = (ax + by + cz + dw)^2 + (ay - bx + dz - cw)^2 + (az - cx + bw - dy)^2 + (aw - dx + cy - bz)^2$$

$\implies$ Es genügt, die Aussage für $p \in \mathbb{P}$ zu verifizieren. $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Sei nun $p \in \mathbb{P}$ ungerade. $0^2, 1^2, \ldots, (\frac{p-1}{2})^2$ sind $\frac{p+1}{2}$ Zahlen, die inkongruent sind $\pmod{p}$. $-0^2 - 1, -1^2 - 1, \ldots, -(\frac{p-1}{2})^2 - 1$ sind $\frac{p+1}{2}$ Zahlen, die inkongruent sind $\pmod{p}$. Zusammen sind dies $p + 1$ Zahlen, die nicht alle inkongruent $\pmod{p}$ sein können.

Daher existieren x, y mit $x^2 \equiv -y^2 - 1 \pmod{p} \iff x^2 + y^2 + 1 + 0 \equiv 0 \pmod{p}$. Wegen $x, y \in \{0, 1, \ldots, \frac{p-1}{2}\}$ gilt $x^2 + y^2 + 1 < p^2$ und daher ist $x^2 + y^2 + 1 = mp$ für ein m mit $0 < m < p$. Sei l die kleinste positive Zahl mit $lp = x^2 + y^2 + z^2 + w^2$. Wir wissen, dass $l \leq m < p$.

Behauptung: l ist ungerade. Wäre l gerade, so wären 0, 2 oder 4 der Summanden in $x^2+y^2+z^2+w^2$ ungerade. OBdA seien $x + y, x - y, z + w, z - w$ gerade. Dann gilt

$$\frac{lp}{2} = \left(\frac{x+y}{2}\right)^2 \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2,$$

ein Widerspruch zu l minimal.

Behauptung: $l = 1$. Seien x', y', z', w' die absolut kleinsten Reste von x, y, z, w bei Division durch l. Dann gilt $\underbrace{x'^2 + y'^2 + z'^2 + w'^2}_{n} \equiv 0 \pmod{l}$. $n > 0$ ($l \nmid p$).

$$l \equiv 1 \pmod{2} \implies n < 4 \cdot \left(\frac{l}{2}\right)^2 = l^2.$$

Daher gilt $n = kl$ mit $0 < k < l$.

Es ist

$$(kl)(lp) = n(x^2 + y^2 + z^2 + w^2) = (x'^2 + y'^2 + z'^2 + w'^2)(x^2 + y^2 + z^2 + w^2) = \square + \square + \square + \square.$$

Jedes $\square$ ist durch l teilbar!

$$\begin{aligned}
\square_1 &= xx' + yy' + zz' + ww' \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{l} \\
\square_2 &= xy' - yx' + zw' - wz' \equiv xy - yx + zw - wz \equiv 0 \pmod{l} \\
\square_3 &= \cdots \equiv 0 \pmod{l} \\
\square_4 &= \cdots \equiv 0 \pmod{l}
\end{aligned}$$

Es folgt: $kp = \square' + \square' + \square' + \square'$, ein Widerspruch zu $k < l$! Also $l = 1, p = x^2 + y^2 + z^2 + w^2$. $\square$

Aufgaben:

1. $2^{2k+1} \neq \square_{>0} + \square_{>0} + \square_{>0} + \square_{>0}$
2. Jedes $n > 169$ ist Summe von 5 Quadraten > 0
3. $n = 4^m(8k + 7) \implies n \neq \square + \square + \square$

1.5 Ternäre quadratische Formen und Summen von 3 Quadraten

Beispiel 1.5.1:

$$\begin{aligned}
3 &= 1^2 + 1^2 + 1^2 \\
5 &= 2^2 + 1^2 + 0^2 \\
15 &\neq \square + \square + \square
\end{aligned}$$

$F = F(x_1, \ldots, x_r) = \sum_{k,l} a_{kl} x_k x_l$ mit $a_{kl} \in \mathbb{Z}, a_{kl} = a_{lk}$. $D(F) := \det((a_{kl})_{1 \leq k,l \leq r})$ heißt Diskriminante von F.

Warnung:

Achtung, das heißt für binäre quadratische Formen, dass

$$D((a, b, c)) = \begin{vmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{vmatrix} = ac - \frac{b^2}{4}.$$

Das ist anders als in Abschnitt 1.3 beziehungsweise Theorem 1.2.3!

$F = \sum_{k,l} a_{kl} x_k x_l \sim G = \sum_{k,l} b_{kl} x_k x_l$ falls $\exists U \in \mathrm{SL}_r(\mathbb{Z})\colon F \circ U = G$. In diesem Fall gilt: $B = U^t A U, b_{kl} = \sum_{m,n} u_{mk} a_{mn} u_{nl}$. $\sim$ ist eine Äquivalenzrelation, äquivalente Formen stellen die selben Zahlen mit den selben Vielfachheiten dar.

Definition 1.5.2:
F heißt positiv definit, falls $F(x_1, \dots, x_r) > 0 \forall (x_1, \dots, x_r) \neq (0, \dots, 0)$.

Proposition 1.5.3:

$$F(x_1, x_2, x_3) = \sum_{k,l=1}^{3} a_{kl} x_k x_l \text{ ist positiv definit} \iff a_{11} > 0 \wedge a_{11} a_{22} - a_{12}^2 > 0 \wedge D(F) > 0$$

Weiters F ist positiv definit $\implies$

$$a_{11} F = (a_{11} x_1 + a_{12} x_2 + a_{13} x_3)^2 + K(x_2, x_3) \tag{1.3}$$

mit K PDBQF mit Diskriminante $a_{11} D(F)$.

Beweis. Mittels direktem Nachrechnen erhält man

$$K(x_2, x_3) = (a_{11} a_{22} - a_{12}^2) x_2^2 + 2(a_{11} a_{23} - a_{12} a_{13}) x_2 x_3 + (a_{11} a_{33} - a_{13}^2) x_3^2$$
$$D(K) = (a_{11} a_{22} - a_{12}^2)^2 (a_{11} a_{33} - a_{13}^2)^2 - (a_{11} a_{23} - a_{12} a_{13})^2 = \cdots = a_{11} D(F)$$

Sei F positiv definit. $a_{11} = F(1, 0, 0) > 0$. Es gilt F ist positiv definit $\iff$ K ist positiv definit! Falls K nicht positiv definit, so existieren x_2, x_3 mit $K(x_2, x_3) \leq 0$ (wobei $(x_2, x_3) \neq (0, 0)$). Dann ist auch $K(\underbrace{a_{11} x_2}_{y_2}, \underbrace{a_{11} x_3}_{y_3}) \leq 0$.

Wähle eine ganzzahlige Lösung von $a_{11} x_1 + a_{12} y_2 + a_{11} y_3 = 0$. Dann ist $F(x_1, y_2, y_3) = K(y_2, y_3) \leq 0$, also ist F nicht positiv definit.

Umgekehrt: ist K positiv definit, so folgt aus Gleichung (1.3) $F(x_1, x_2, x_3) \geq K(x_2, x_3)$. Falls $(x_2, x_3) \neq (0, 0)$, so ist $F > 0$. Falls $x_2 = x_3 = 0$, so ist $x_1 \neq 0$ und $F(x_1, 0, 0) = a_{11} x_1^2 > 0$.

K ist positiv definit $\iff \begin{cases} a_{11} D(F) > 0 \\ a_{11} a_{22} - a_{12}^2 > 0 \end{cases}$, was zu zeigen war. □

Lemma 1.5.4:

Für

$$U = \begin{pmatrix} u_{11} & * & * \\ u_{21} & * & * \\ u_{31} & * & * \end{pmatrix}$$

mit $\mathrm{ggT}(u_{11}, u_{21}, u_{31}) = 1$ existieren 6 weitere Einträge, sodass $U \in SL_3(\mathbb{Z})$ ist.

Beweis. Sei $g = \mathrm{ggT}(u_{11}, u_{21})$. Dann ist $\mathrm{ggT}(g, u_{31}) = 1$. $\exists u_{12}, u_{22}$, sodass $u_{11}u_{22} - u_{12}u_{21} = g$ und $\exists s, t$ sodass $gs - u_{31}t = 1$. Setze $U := \begin{pmatrix} u_{11} & u_{12} & \frac{u_{11}t}{g} \\ u_{21} & u_{22} & \frac{u_{21}t}{g} \\ u_{31} & 0 & s \end{pmatrix}$. Durch Entwickeln nach der 1. Spalte erhalten wir $U \in \mathrm{SL}_3(\mathbb{Z})$. □

Satz 1.5.5:

Jede Äquivalenzklasse PDTQF enthält eine Form mit

$$a_{11} \leq \frac{4}{3}\sqrt[3]{D(F)},\ 2\,|a_{12}| \leq a_{11},\ 2\,|a_{13}| \leq a_{11}.$$

Beweis. Sei F eine PDTQF. Wähle a_{11} als die kleinste positive von einer zu F äquivalenten Form dargestellte Zahl. Dann sei (u_{11}, u_{21}, u_{31}) eine Lösung von $F(x_1, x_2, x_3) = a_{11}$. Die Minimalität von a_{11} garantiert $\mathrm{ggT}(u_{11}, u_{21}, u_{31}) = 1$. Mit Theorem 1.5.4, wähle ein $U \in \mathrm{SL}_3(\mathbb{Z})$ mit $U = \begin{pmatrix} u_{11} & * & * \\ u_{21} & * & * \\ u_{31} & * & * \end{pmatrix}$.

Setze $G := F \circ U$. Mit $G = \sum b_{kl}x_kx_l$ folgt $b_{11} = G(1,0,0) = F \circ U(1,0,0) = F(u_{11}, u_{21}, u_{31}) = a_{11}$. Setze nun $D := \begin{pmatrix} 1 & r & s \\ 0 & t & u \\ 0 & v & w \end{pmatrix}$ mit $tw - uv = 1$ und setze $H := G \circ D$, $H(y_1, y_2, y_3) := \sum_{k,l} a_{kl}y_ky_l$.

Es gilt

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ r & t & v \\ s & u & w \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} \begin{pmatrix} 1 & r & s \\ 0 & t & u \\ 0 & v & w \end{pmatrix}$$

$$\Longrightarrow \begin{cases} a_{11} = a_{11} \cdot 1 \\ a_{12} = a_{11} \cdot r + b_{12} \cdot t + b_{12} \cdot v \\ a_{13} = a_{11} \cdot s + b_{12} \cdot u + b_{13} \cdot w \end{cases}$$

und $H = G \circ D$ impliziert

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = D \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

$$\begin{pmatrix} b_{11} & b_{12} & b_{13} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} & b_{13} \end{pmatrix} D \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

Aus Gleichung (1.3) folgt:

$$\begin{aligned} a_{11} G &= (b_{11}x_1 + b_{12}x_2 + b_{13}x_3)^2 + K(x_2, x_3) \\ a_{11} H &= (a_{11}y_1 + a_{12}y_2 + a_{13}y_3)^2 + L(y_2, y_3) \end{aligned}$$

mit PDBQF K und L.

$$a_{11}(G(x_1, x_2, x_3) - H(y_1, y_2, y_3)) = K(x_2, x_3) - L(y_2, y_3).$$

Mit $H = G \circ D$ folgt, dass $K \circ \begin{pmatrix} t & u \\ v & w \end{pmatrix} = L$. Insbesondere ist $K \sim L$ als PDBQF. Bezeichnet d die Diskriminante von F (und G, H), so hat L die Diskriminante $a_{11}d$ und führenden Koeffizienten $a_{11}a_{22} - a_{12}^2$. Wähle nun t, u, v, w so, dass L als PDBQF reduziert ist.

Behauptung: $a_{11}a_{22} - a_{12}^2 \leq \frac{2}{\sqrt{3}}\sqrt{a_{11}d}$.

($f = (a, b, c)$ mit Diskriminante d reduziert, dann ist $|b| \leq a \leq c$ Es folgt: $a^2 \leq ac = d + \frac{b^2}{4} \leq d + \frac{a^2}{4} \implies \frac{3}{4}a^2 \leq d \iff \frac{\sqrt{3}}{2}a \leq \sqrt{d} \iff \frac{2}{\sqrt{3}}\sqrt{d} \geq a$)

$$\begin{aligned} a_{12} &= a_{11}r + \underbrace{tb_{12} + vb_{13}}_{=:m} \\ a_{13} &= a_{11}s + \underbrace{ub_{12} + wb_{13}}_{=:n} \end{aligned}$$

Wähle r, s so, dass $|a_{12}| \leq \frac{a_{11}}{2}, |a_{13}| \leq \frac{a_{11}}{2}$. a_{12}, a_{13} liegen in den Restklassen $m, n \pmod{a_{11}}$, wir wählen die minimalen Vertreter dieser Restklassen. $H(0, 1, 0) = a_{22} \geq a_{11}$ aufgrund der Wahl von a_{11} als kleinster von einer zu F äquivalenten Form dargestellten, positiven Zahl.

$$a_{11}^2 \leq a_{11}a_{22} = (a_{11}a_{22} - a_{12}^2) + a_{12}^2 \leq \frac{2}{\sqrt{3}}\sqrt{a_{11}d}$$

Durch Umformen ergibt sich $a_{11} \leq \frac{4}{3}\sqrt[3]{d}$, was zu zeigen war. □

Korollar 1.5.6:

Jede PDTQF mit Diskriminante 1 ist zu $x_1^2 + x_2^2 + x_3^2$ äquivalent.

Beweis. Jede solche ist zu einer Form mit den Eigenschaften aus Theorem 1.5.5 äquivalent. $a_{11} \leq \frac{4}{3} \implies a_{11} = 1, a_{12} = 0, a_{13} = 0$, also $F(x_1, x_2, x_3) = x_1^2 + K(x_2, x_3)$ mit $K(x_2, x_3) = a_{22}x_2^2 + 2a_{23}x_2x_3 + a_{33}x_3^2$. K hat Diskriminante 1 (-4 in Abschnitt 1.3) und ist daher äquivalent zu $x_2^2 + x_3^2$ via $U = \begin{pmatrix} t & u \\ v & w \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Dann ist $F \sim x_1^2 + x_2^2 + x_3^2$ mittels Verknüpfung mit $\begin{pmatrix} 1 & 0 & 0 \\ 0 & t & u \\ 0 & v & w \end{pmatrix}$. □

Satz 1.5.7:

Jedes $n \in \mathbb{N}$, das nicht von der Form $n = 4^m \cdot (8k + 7)$ ist, lässt sich als Summe von 3 Quadraten schreiben.

Beweis. $n = \square + \square + \square \implies 4n = \square + \square + \square$. Sei oBdA $n \not\equiv 0 \pmod 4$, sodass $n \equiv 1, 2, 3, 5, 6 \pmod 8$. Wegen Theorem 1.5.6 genügt es, für jedes dieser n eine PDTQF der Diskriminante 1 zu finden, die n darstellt.

Bestimme $a_{11}, a_{12}, a_{22}, a_{13}, a_{23}, a_{33}, x_1, x_2, x_3$ mit:

- $a_{11}x_1^2 + 2_a12x_1x_2 + a_{22}x_2^2 + 2a_{13}x_1x_32a_{23}x_2x_3 + a_{33}x_3^2 = n$
- $a_{11} > 0$
- $\underbrace{a_{11}a_{22} - a_{12}^2}_{=:b} > 0$
- $\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = 1$

Wir legen sofort 6 der Unbekannten fest: $a_{13} = 1, a_{23} = 0, a_{33} = n, x_1 = x_2 = 0, x_3 = 1$. Dies garantiert, dass n von der Form dargestellt wird ($\iff$ 1. Bedingung).

$n = 1 \;\; 1 = 1 + 0 + 0$ ✓. $a_{11} > 0$ folgt aus: $n > 1$ und $\begin{vmatrix} a_{11} & a_{12} & 1 \\ a_{21} & a_{22} & 0 \\ 1 & 0 & n \end{vmatrix} = bn - a_{22} = 1$

$$a_{22} = bn - 1 > b - 1 \geq 0$$
$$a_{11}a_{22} = b + a_{12} > 0$$

Es verbleiben 2 Bedingungen: um diese zu erfüllen, müssen wir ein $b > 0$ bestimmen, für das:

$$\begin{aligned} a_{11} = \frac{b + a_{12}^2}{a_{22}} \in \mathbb{Z} &\iff b + a_{12}^2 \equiv 0 \pmod{a_{22}} \\ &\iff -b \text{ Quadratischer Rest} \pmod{a_{22}} \\ &\iff -b \text{ Quadratischer Rest} \pmod{bn - 1} \end{aligned}$$

Wir unterscheiden 2 Fälle:

1. $n \equiv 2, 6 \pmod 8$. Behauptung: wir können b so wählen, dass $bn - 1 =: p$ eine Primzahl ist, für die $(\frac{-b}{p}) = 1$. Wir wählen dazu eine Primzahl p aus der arithmetischen Progression $(n-1) + 4nt$. Die Existenz ist durch Theorem 3.5.6 gegeben. Setze $b = 4t + 1, p = bn - 1$. Wegen $n \equiv 2 \pmod 4, b \equiv 1 \pmod 4$ folgt $p \equiv 1 \pmod 4$.

$$\left(\frac{-b}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{b}{p}\right) = \left(\frac{p}{b}\right) = \left(\frac{bn-1}{b}\right) = \left(\frac{-1}{b}\right) = 1.$$

2. $n \equiv 1, 3, 5 \pmod 8$. Setze $c := \begin{cases} 3 & \text{für } n \equiv 1, 5 \pmod 8 \\ 1 & \text{für } n \equiv 3 \pmod 8 \end{cases}$. In jedem Fall ist $\frac{cn-1}{2}$ ungerade, $\mathrm{ggT}(\frac{cn-1}{2}, 4n) = 1$. Die arithmetische Progression $\frac{cn-1}{2} + 4nt$ enthält daher eine Primzahl p. Für diese ist $p = \frac{1}{2}((8t + c)n - 1)$, $b = 8t - c$ und $2p = bn - 1$. b ist ungerade.

$$\begin{aligned} n \equiv 1 \pmod 8 &\implies b \equiv 3 \pmod 8, p \equiv 1 \pmod 4 \\ n \equiv 3 \pmod 8 &\implies b \equiv 1 \pmod 8, p \equiv 1 \pmod 4 \\ n \equiv 5 \pmod 8 &\implies b \equiv 3 \pmod 8, p \equiv 3 \pmod 4 \end{aligned}$$

$\implies$ in jedem Fall ist $\frac{p-1}{2}\frac{b+1}{2}$ gerade. Zudem gilt $(\frac{-2}{b}) = (\frac{-1}{b})(\frac{2}{b}) = 1$.

$$\left(\frac{-b}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{b}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{b-1}{2}}\left(\frac{p}{b}\right) = \overbrace{(-1)^{\frac{p-1}{2}\cdot\frac{b+1}{2}}}^{=1}\left(\frac{p}{b}\right)$$
$$= \left(\frac{p}{b}\right) = \left(\frac{p}{b}\right)\left(\frac{-2}{b}\right) = \left(\frac{-2p}{b}\right) = \left(\frac{1-nb}{b}\right) = \left(\frac{1}{b}\right) = 1$$

Also ist $-b$ quadratischer Rest $\pmod p$, da b ungerade ist, folgt $-b$ quadratischer Rest $\pmod{2p}$, also $\pmod{bn-1}$. □

2 Quadratische Formen über $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}_p$

2.1 p-adische Zahlen

$x^2 \equiv 2 \pmod 7 \dots x^2 \pmod{7^k}$. $x^2 \equiv 2 \pmod 7$ hat Lösungen $3, -3$ in $\mathbb{Z}/7\mathbb{Z}$. Setze $x_0 = 3$. Gesucht: $x_1 \in \mathbb{Z}$ mit $x_1^2 \equiv 2 \pmod{7^2}$ mit $x_1 \equiv x_0 \pmod 7$, das heißt $x_1 = x_0 + 7a_1$ mit $a_1 \in \mathbb{Z}$.

$$\begin{aligned}(x_0 + 7a_1)^2 \equiv 2 \pmod{7^2} &\iff x_0^2 + 2 \cdot 7a_1x_0 + 7^2a_1^2 \equiv 2 \pmod{7^2} \\ &\iff (x_0^2 - 2) + 7 \cdot 2a_1x_0 \equiv 0 \pmod{7^2} \\ &\iff 7 + 7 \cdot 6a_1 \equiv 0 \pmod{7^2} \\ &\iff 1 + 6a_1 \equiv 0 \pmod 7 \iff a_1 \equiv 1 \pmod 7\end{aligned}$$

Also $x_1 = 3 + 1 \cdot 7$ ist Lösung von $x^2 - 2 \equiv 0 \pmod{49}$.

Allgemein: sei $x_k = \sum_{i=0}^{k} a_i 7^i$ eine Lösung von $x^2 - 2 \equiv 0 \pmod{7^{k+1}}$. Gesucht ist x_{k+1} mit $x_{k+1}^2 - 2 \equiv 0 \pmod{7^{k+2}}$ und $x_{k+1} \equiv x_k \pmod{7^{k+1}}$. Schreibe $x_{k+1} = x_k + a_{k+1}7^{k+1}$.

$$\begin{aligned}(x_k + 7^{k+1}a_{k+1})^2 - 2 &\equiv x_k^2 + 2 \cdot 7^{k+1}a_{k+1}x_k + 7^{2k+2}a_{k+1}^2 - 2 \pmod{7^{k+2}} \\ 0 &\equiv \underbrace{(x_k^2 - 2)}_{7^{k+1}b_{k+1}} + 2a_{k+1}7^{k+1}x_k \pmod{7^{k+2}} \\ \iff 0 &\equiv b_{k+1} + 2a_{k+1}\underbrace{x_k}_{\equiv x_0 \pmod 7} \pmod 7 \\ \iff 0 &\equiv b_{k+1} + 6a_{k+1} \pmod 7 \\ \iff a_{k+1} &\equiv -b_{k+1}\underbrace{6^{-1}}_{-1} \equiv b_{k+1} \pmod 7\end{aligned}$$

$\implies$ eindeutige Fortsetzung von $x_k \pmod{7^{k+1}}$ ist $x_{k+1} = \sum_{i=0}^{k+1} a_i 7^i$.

Hier:

$$\begin{aligned}x_0 &= 3 \\ x_1 &= 3 + 1 \cdot 7 = 10 \\ x_2 &= 3 + 1 \cdot 7 + 2 \cdot 7^2 = 108 \\ x_3 &= 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 = 2166 \\ x_4 &= 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 1 \cdot 7^4 = \dots\end{aligned}$$

Definition 2.1.1:

Für $p \in \mathbb{P}$ heißt

$$\mathbb{Z}_p := \left\{ (\bar{x}_k) \in \prod_{k=0}^{\infty} \left(\mathbb{Z}/p^{k+1}\mathbb{Z} \right) : x_{k+1} \equiv x_k \pmod{p^{k+1}} \right\}$$

mit der komponentenweisen Addition und Multiplikation, $0 := (\bar{0})_k$, $1 := (\bar{1})_k$ der Ring der p-adischen ganzen Zahlen.

Es ist $\varepsilon_p \colon \mathbb{Z} \to \mathbb{Z}_p$ eine Einbettung.
$n \mapsto (\bar{n}, \bar{n}, \dots)$

Beispiel 2.1.2:

$p = 7$

$$\begin{aligned} \varepsilon_7(173) &= (\overline{173}, \overline{173}, \dots) = (5, 26, 173, 173, \dots) \\ \varepsilon_7(-1) &= (\overline{-1}, \overline{-1}, \dots) = (6, 48, 342, \dots, 7^k - 1) \\ \sqrt{\varepsilon_7(2)} &= (3, 10, 108, 2166, \dots) \end{aligned}$$

$x = (\bar{x}_k)$ heißt reduziert, falls $0 \le x_k < p^{k+1}$. Alternativ verwenden wir die Potenzreihendarstellung:

$$x = \sum_{i=0}^{\infty} a_i p^i$$

mit $0 \le a_i < p$.

$$\varepsilon_7(-1) = 6 + 6 \cdot 7 + 6 \cdot 7^2 + \dots$$

$\mathbb{Z}_p$ $x = (x_0, x_1, x_2, \dots)$ mit $x_k \in \mathbb{Z}/p^{k+1}\mathbb{Z}$ und $x_{k+1} \equiv x_k \pmod{p^{k+1}}$ mit $a_k = \frac{x_{k+1} - x_k}{p^{k+1}}$ folgt $x = a_0 p^0 + a_1 p^1 + a_2 p^2 + \cdots$ mit $0 \le a_i < p$.

Beispiel 2.1.3:

$$\begin{aligned} (3 \cdot 7^0 + 4 \cdot 7^1 + 2 \cdot 7^2) + (5 \cdot 7^0 + 3 \cdot 7^1) &= (3+5)7^0 + (4+3)7^1 + 2 \cdot 7^2 \\ &= 1 \cdot 7^0 + 1 \cdot 7^1 + 3 \cdot 7^2 \end{aligned}$$

$$\begin{aligned} (3 \cdot 7^0 + 4 \cdot 7^1 + 2 \cdot 7^2) \cdot (5 \cdot 7^0 + 3 \cdot 7^1) = {} & (3 \cdot 5)7^0 + (3 \cdot 3 + 4 \cdot 5)7^1 \\ & + (4 \cdot 3 + 2 \cdot 5)7^2 + (2 \cdot 3)7^3 \\ = {} & 1 \cdot 7^0 + 3 \cdot 7^1 + 5 \cdot 7^2 + 2 \cdot 7^3 + 1 \cdot 7^4 \end{aligned}$$

Satz 2.1.4:

1. $\mathbb{Z}_p$ ist HIB.
2. $\varepsilon_p \colon \mathbb{Z} \to \mathbb{Z}_p$ ist eine Einbettung.
   $x \mapsto (x, x, \dots)$
3. $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus p\mathbb{Z}_p$
4. Für $x \in \mathbb{Z}_p \setminus \{0\}$: $x = p^n \cdot u$ mit $u \in \mathbb{Z}_p^*$, $n \in \mathbb{N}$ eindeutig. Insbesondere ist p das einzige Primelement in $\mathbb{Z}_p$.
5. $I \trianglelefteq \mathbb{Z}_p \implies I = (0) \vee I = p^n\mathbb{Z}_p$ mit $n \geq 1$. Es gilt:
$$\bigcap_{n\geq 1} p^n\mathbb{Z}_p = (0), \quad {}^{\mathbb{Z}_p}\!/_{p^n\mathbb{Z}_p} \cong {}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}}.$$

Beweis.

1. Zeigen $\mathbb{Z}_p$ ist IB, HIB folgt dann aus Punkt 5. Seien $x = (x_k), y = (y_k) \neq 0$. Zu Zeigen: $z = xy = (x_k y_k) \neq 0$. $\exists m, n \colon x_n \not\equiv 0 \pmod{p^{n+1}}, y_m \not\equiv 0 \pmod{p^{m+1}}$. Sei $l = m + n$. Nach Definition gilt: $x_l \equiv x_n \pmod{p^{n+1}}$ und $y_l \equiv x_m \pmod{p^{m+1}}$. $\implies x_l = u \cdot p^{n'}$ mit $(u, p) = 1$ und $n' \leq n$.

   $y_l = v \cdot p^{m'}$ mit $m' \leq m$. Es ist $m' + n' \leq l$ und $z_l = uvp^{m'+n'} \not\equiv 0 \pmod{p^{l+1}}$, das heißt $z \neq 0$.

2. klar.

3. $x \in p\mathbb{Z}_p$ kann keine Einheit sein, denn dann ist $x_0 \equiv 0 \pmod{p}$ und daher gilt für jedes $y \in \mathbb{Z}_p$: $(xy)_0 = 0$, im Widerspruch zu $xy = (1, 1, \dots)$.

   Umgekehrt, sei $x \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Dann ist $x_0 \not\equiv 0 \pmod{p}$ Daher ist $x_k \equiv x_0 \pmod{p}$ und folglich $x_k \in \left({}^{\mathbb{Z}}\!/_{p^{k+1}\mathbb{Z}}\right)^*$. Daher existiert $y_k := x_k^{-1}$ in ${}^{\mathbb{Z}}\!/_{p^{k+1}\mathbb{Z}}$ und wir setzen $y = (y_k)$.

   Behauptung: $y_{k+1} \equiv y_k \pmod{p^{k+1}}$. Nach Definition gilt $x_{k+1} \cdot y_{k+1} \equiv 1 \pmod{p^{k+2}}$ und $x_{k+1} \equiv x_k \pmod{p^{k+1}}$. Es folgt: $x_k \cdot y_{k+1} \equiv 1 \pmod{p^{k+1}}$. Andererseits gilt nach Definition: $x_k \cdot y_k \equiv 1 \pmod{p^{k+1}}$. Daraus folgt die Behauptung.

4. Sei $x = (x_k) \in p^n\mathbb{Z}_p \implies x_k = 0$ in ${}^{\mathbb{Z}}\!/_{p^{k+1}\mathbb{Z}}$ für $k < n$ sodass $\bigcap_{n\geq 1} p^n\mathbb{Z}_p = \{0\}$. Für $x \neq 0$ in $\mathbb{Z}_p$ gilt daher: $\exists n \colon x \in p^n\mathbb{Z}_p \setminus p^{n+1}\mathbb{Z}_p$. Daher ist $x = p^n \cdot u$ mit $u \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$, wobei n eindeutig festgelegt ist. Nach Punkt 1 folgt: auch u ist eindeutig bestimmt.

   Behauptung: p ist prim, das heißt $p \mid xy \implies p \mid x \vee p \mid y$. Aus $p \mid xy$ folgt: $xy \in p\mathbb{Z}_p \iff xy \notin \mathbb{Z}_p^*$. Es folgt: $x \notin \mathbb{Z}_p^* \vee y \notin \mathbb{Z}_p^*$, das heißt $x \in p\mathbb{Z}_p \vee y \in p\mathbb{Z}_p$. Aus der Darstellung $x = p^n \cdot u$ mit $u \in \mathbb{Z}_p^*$ für alle $x \in \mathbb{Z}_p$ folgt, dass es kein weiteres Primelement geben kann.

5. Sei $I \trianglelefteq \mathbb{Z}_p$. Aus $\bigcap_{n\geq 1} p^n\mathbb{Z}_p = \{0\}$ folgt $\bigcap_{n\geq 1}(p^n\mathbb{Z}_p \cap I) = \{0\}$. $I = I \cap p^0\mathbb{Z}_p$ und daher existiert ein minimales n mit

$$I \cap p^n\mathbb{Z}_p = I \tag{2.1}$$

und $I \cap p^{n+1}\mathbb{Z}_p \subsetneq I$.

Behauptung: $I = p^n\mathbb{Z}_p$.

$$I \cap p^{n+1}\mathbb{Z}_p \subsetneq I \implies \exists x\colon x \in I, x \notin I \cap p^{n+1}\mathbb{Z}_p.$$

Dieses x hat die Gestalt $u \cdot p^n$ mit $u \in \mathbb{Z}_p^*$. Es folgt: $p^n \in I$ und somit $p^n\mathbb{Z}_p \subseteq I$. Wegen Gleichung (2.1) gilt auch $p^n\mathbb{Z}_p \supseteq I$, insgesamt also $p^n\mathbb{Z}_p = I$.

Sei Π die kanonische Projektion $\prod_k {}^{\mathbb{Z}}\!/_{p^{k+1}\mathbb{Z}} \to {}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}}$. Die Einschränkung $\tilde{\Pi}$ von Π auf $\mathbb{Z}_p$ ist surjektiv: für $x_{n-1} \in {}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}}$ ist $\Pi(x_{n-1}, \dots) = x_{n-1}$.

$$\ker\tilde{\Pi} \trianglelefteq \mathbb{Z}_p \implies \ker\tilde{\Pi} = p^l\mathbb{Z}_p \vee \ker\tilde{\Pi} = (0).$$

$\Pi(p^k) = 0 \iff k \leq n$, sodass $\ker\tilde{\Pi} = p^n\mathbb{Z}_p$ (das heißt $l = n$). Mit dem Homomorphiesatz folgt die Behauptung. □

Definition 2.1.5:

$$\mathbb{Q}_p = \left\{\frac{r}{s}\colon r \in \mathbb{Z}_p, s \in \mathbb{Z}_p \setminus \{0\}\right\}$$

als Quotientenkörper von $\mathbb{Z}_p$ heißt Körper der p-adischen Zahlen.

Nach Theorem 2.1.4 gilt

$$\mathbb{Q}_p = \left\{\frac{r}{p^n}\colon r \in \mathbb{Z}_p, n \in \mathbb{N}\right\} = \{p^n \cdot u\colon u \in \mathbb{Z}_p^*, n \in \mathbb{Z}\}.$$

ε_p setzt sich zu einer Einbettung von $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ folgt, dass die Darstellung $x = p^n \cdot u$ mit $u \in \mathbb{Z}_p^*, n \in \mathbb{Z}$ weiterhin eindeutig ist.

Definition 2.1.6:

Die p-adische Bewertung ν_p auf $\mathbb{Q}_p$ ist definiert durch

$$\begin{aligned} \mathbb{Q}_p &\to \mathbb{Z} \cup \{\infty\} \\ \nu_p\colon p^n \cdot u &\mapsto n \\ 0 &\mapsto \infty. \end{aligned}$$

Lemma 2.1.7:

(1) $\nu_p(x) = \infty \iff x = 0$.
(2) $\nu_p(xy) = \nu_p(x) + \nu_p(y)$.
(3) $\nu_p(x+y) \geq \min\{\nu_p(x), \nu_p(y)\}$. Falls $\nu_p(x) \neq \nu_p(y)$, gilt sogar $\nu_p(x+y) = \min\{\nu_p(x), \nu_p(y)\}$.
(4) $x \in \mathbb{Z}_p \iff \nu_p(x) \geq 0$.
(5) $x \in \mathbb{Z}_p^* \iff \nu_p(x) = 0$.

Beweis. Punkte 2.1.7 (1) und 2.1.7 (2) folgen unmittelbar aus der Definition.

3. Ist $x = 0 \vee y = 0$, so ist nichts zu zeigen. Für $x = p^n \cdot u, y = p^m \cdot v$ mit oBdA $n \leq m$.

$$x + y = p^n u + p^m v = p^n (\underbrace{u + p^{\overbrace{m-n}^{\geq 0}} v}_{\in \mathbb{Z}_p}) \implies \nu_p(x+y) \geq n = \nu_p(x) = \min\{\nu_p(x), \nu_p(y)\}.$$

Falls $\nu_p(x) \neq \nu_p(y)$, das heißt $m \neq n$, so ist $u + p^{m-n} v \in \mathbb{Z}_p^*$, das heißt $\nu_p(x+y) = n = \nu_p(x) = \min\{\nu_p(x), \nu_p(y)\}$. □

Bemerkung 2.1.8:

Die Punkte 2.1.7 (1) bis 2.1.7 (3) charakterisieren Bewertungen auf einem Körper. Die Abbildung $\nu \colon K \to \mathbb{Z} \cup \{\infty\} \colon \nu(x) = 0 \forall x \in K \setminus \{0\}, \nu(0) = \infty$ heißt die triviale Bewertung auf K.

Definition 2.1.9:

Auf $\mathbb{Q}_p$ definiert $|.|_p : \mathbb{Q}_p \to \mathbb{R}$, definiert durch $x \mapsto p^{-\nu_p(x)}$ einen Absolutbetrag (Norm).

Lemma 2.1.10:

1. $|x|_p \geq 0 \wedge |x|_p = 0 \iff x = 0$.
2. $|xy|_p = |x|_p \, |y|_p$.
3. $|x+y|_p \leq \max\{|x|_p, |y|_p\}$. Falls $|x|_p \neq |y|_p$, so gilt sogar $|x+y|_p = \max\{|x|_p, |y|_p\}$.
4. $x \in \mathbb{Z}_p \iff |x|_p \leq 1$.
5. $x \in \mathbb{Z}_p^* \iff |x|_p = 1$.

Bemerkung 2.1.11:

- Die Punkte 1 bis 3 charakterisieren Absolutbeträge auf Körpern.
- Der p-adische Absolutbetrag auf $\mathbb{Q}_p$ ist nicht-archimedisch (das heißt $|n \cdot 1|_p \leq 1$ für alle $n \in \mathbb{N}$).

$x \in \mathbb{Q}_p \colon x = p^n u \to \nu_p(x) = n \; |x|_p := p^{-\nu_p(x)} = p^{-n}$

Satz 2.1.12:

$\mathbb{Q}_p$ ist bezüglich $|\cdot|_p$ vollständig, das heißt jede Cauchy Folge konvergiert.

Beweis. OBdA bestehe die Cauchyfolge $(x_i)_{i\in\mathbb{N}}$ aus Elementen von $\mathbb{Z}_p$. $\{|x_i|_p : i \in \mathbb{N}\}$ ist nach oben beschränkt: sonst gäbe es für $m \in \mathbb{N}$ ein $N \in \mathbb{N}$: $i, j > N$: $|x_i|_p > |x_j|_p > p^m$. Wegen $|x_i - x_j|_p = |x_i|_p > p^m$, im Widerspruch zu x_i Cauchyfolge.

Wähle $m \in \mathbb{N}$ mit $m > \max\{|x_i|_p : i \in \mathbb{N}\}$ ersetzen wir $(x_i)_{i\in\mathbb{N}}$ durch $(p^m x_i)_{i\in\mathbb{N}}$. Sei nun $(x_i)_{i\in\mathbb{N}}$ eine Cauchyfolge aus $\mathbb{Z}_p$. Für $k \in \mathbb{N}$ wähle N_k so, dass $|x_i - x_j|_p < p^{-k}$ für $i, j \geq N_k$. OBdA sei N_k monoton wachsend.

$$|x_i - x_j| < p^{-k} \iff \nu_p(x_i - x_j) > k \iff x_i - x_j \in p^{k+1}\mathbb{Z}_p.$$

Wähle nun $z_k \in \mathbb{Z}$ mit $z_k \equiv x_i \equiv x_j \pmod{p^{k+1}}$ (für $i, j \geq N_k$). Wegen $N_{k+1} > N_k$ gilt $z_{k+1} \equiv z_k \pmod{p^{k+1}}$, das heißt (z_k) bestimmt eindeutig eine p-adische ganze Zahl z.

Für $i \geq N_k$ gilt $x_i \equiv z_k \equiv z \pmod{p^{k+1}}$, also $|x_i - z| < p^{-k}$, also $x_i \overset{i\to\infty}{\to} z$. □

Auf $\mathbb{Q}$ kann $|\cdot|_p$ auch definiert werden als

$$\left|\frac{a}{b}\right|_p = p^{\beta-\alpha}$$

wobei $p^\alpha \mid\mid a$ und $p^\beta \mid\mid b$. $\mathbb{Q}_p$ ist dann die Vervollständigung von $\mathbb{Q}$ bezüglich $|\cdot|_p$. (Äquivalenzklassen von Cauchyfolgen)

Definition 2.1.13:

Zwei Absolutbeträge $|\cdot|$ und $\|\cdot\|$ auf einem Körper K heißen äquivalent, falls $\exists c, C > 0$ mit

$$c \cdot \|\cdot\| \leq |\cdot| \leq C \cdot \|\cdot\|.$$

Satz 2.1.14 (Satz von Ostrowski):
Jeder nicht-triviale Absolutbetrag auf $\mathbb{Q}$ ist zu $|\cdot|$ oder $|\cdot|_p$, $p \in \mathbb{P}$ äquivalent.

Satz 2.1.15 (Produktformel):
Für alle $x \in \mathbb{Q} \setminus \{0\}$ gilt

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} |x|_p = 1.$$

Dabei ist $|\cdot|_\infty = |\cdot|$.

Beweis. Schreibe $x = \pm \prod_{p \in \mathbb{P}} p^{e_p(x)}$ mit $e_p(x) \in \mathbb{Z}, e_p(x) = 0$ für alle bis auf endlich viele p.

$$|x|_\infty = \prod_{p \in \mathbb{P}} p^{e_p(x)}, |x|_p = p^{-e_p(x)},$$

sodass das Produkt 1 ergibt. □

Zurück zum Lösen polynomialer Gleichungen:

Lemma 2.1.16:
Sei $f \in \mathbb{Z}_p[x]$ und $\tilde{x} \in \mathbb{Z}_p$ mit $f(\tilde{x}) \equiv 0 \pmod{p^k}$. Für $a \in \mathbb{Z}, l \leq k$ gilt

$$f(\tilde{x} + ap^k) \equiv 0 \pmod{p^{k+l}} \iff f'(\tilde{x}) \cdot a \equiv \frac{-f(\tilde{x})}{p^k} \pmod{p^l}.$$

Beweis. Entwickle f als Taylorreihe um $\tilde{x}$: $f(x) = \sum_{i=0}^{d} x_i (x - \tilde{x})^i$ mit $c_i \in \mathbb{Z}_p$. Es ist $c_0 = f(\tilde{x}), c_1 = f'(\tilde{x})$.

$$f(\tilde{x} + ap^k) = \sum_{i=0}^{d} c_i (ap^k)^i = f(\tilde{x}) + f'(\tilde{x}) ap^k + p^{2k} \sum_{i=2}^{d} c_i a^i p^{i(k-2)}$$
$$\equiv f(\tilde{x}) + f'(\tilde{x}) ap^k \pmod{p^{k+l}}.$$

Daher ist

$$\begin{aligned} f(\tilde{x} + ap^k) \equiv 0 \pmod{p^{k+l}} &\iff f(\tilde{x}) + f'(\tilde{x}) ap^k \equiv 0 \pmod{p^{k+l}} \\ &\iff \left(\frac{f(\tilde{x})}{p^k} + f'(\tilde{x}) a\right) p^k \equiv 0 \pmod{p^{k+l}} \\ &\iff \frac{-f(\tilde{x})}{p^k} \equiv a f'(\tilde{x}) \pmod{p^l}. \end{aligned}$$

□

Lemma 2.1.17 (Lemma von Hensel):
Sei $f \in \mathbb{Z}_p[x]$ ein Polynom $\tilde{x} \in \mathbb{Z}_p$ mit $f(\tilde{x}) \equiv 0 \pmod{p}, f'(\tilde{x}) \not\equiv 0 \pmod{p}$. Dann existiert ein eindeutig bestimmtes $x \in \mathbb{Z}_p$ mit $f(x) = 0$ und $x \equiv \tilde{x} \pmod{p}$. (Jede einfache Nullstelle von $f \pmod{p}$ kann geliftet werden zu einer einfachen Nullstelle von f in $\mathbb{Z}_p$.)

Wir zeigen eine weniger allgemeine Formulierung:

Satz 2.1.18:
Sei $f \in \mathbb{Z}_p[x]$ und $\tilde{x} \in \mathbb{Z}_p$ mit $f(\tilde{x}) \equiv 0 \pmod{p^{2l+1}}$ und $\nu_p(f'(\tilde{x})) = l$. Dann existiert ein eindeutig bestimmtes $x \in \mathbb{Z}_p$ mit $f(x) = 0$ und $x \equiv \tilde{x} \pmod{p^{l+1}}$.

Beweis. Wir konstruieren $x \in \mathbb{Z}_p$ als Folge (x_k) mit $x_k \in \mathbb{Z}$ mit

- $x_k \equiv \tilde{x} \pmod{p^{\min\{l+1,k+1\}}}$
- $x_k \equiv x_{k-1} \pmod{p^k}$
- $f(x_k) \equiv 0 \pmod{p^{k+l+1}}$

$\exists z \in \mathbb{Z}$ mit $z \equiv \tilde{x} \pmod{p^{2l+1}}$. Setze $x_o = x_1 = \cdots = x_l = z$. Sei $x_{k-1} (k - 1 \geq l)$ schon bestimmt. Setze $x_k := x_{k-1} + ap^k$ mit $a \in \mathbb{Z}$. Nach dem Theorem 2.1.16:

$$f(x_k) \equiv f(x_{k+1} + ap^k)(p^{k+l+1}) \iff f'(x_{k-1})a \equiv \frac{-f(x_{k-1})}{p^k} \pmod{p^{l+1}}. \tag{2.2}$$

Wir wissen, dass nach Konstruktion $x_{k-1} \equiv \tilde{x} \pmod{p^{l+1}} \implies f'(x_{k-1}) \equiv f'(\tilde{x}) \pmod{p^{l+1}}$ und daher $f'(x_{k-1}) \equiv 0 \pmod{p^l}$ und $f'(x_{k-1}) \not\equiv 0 \pmod{p^{l+1}}$. Daher gilt: $\nu_p(f'(x_{k-1})) = l$.

$f(x_{k-1}) \equiv 0 \pmod{p^{k+l}}$ nach Annahme $\implies p^k f'(x_{k-1}) \mid f(x_{k-1})$. $a \equiv \frac{-f(x_{k-1})}{f'(x_{k-1})p^k}$ ist daher die eindeutige Lösung von Gleichung (2.2).

Es folgt: $x_k \equiv x_{k-1} + ap^k \pmod{p^{k+1}}$ (eindeutig, da a eindeutig). Mit $x := (x_k)$ haben wir eine Nullstelle von f. □

2.2 Quadratrestklassen und das Hilbertsymbol

$x^2 - d$ in $\mathbb{Z}_p$.

Für einen Körper K sei $(K^*)^2 := \{a^2 : a \in K^*\}$. $(K^*)^2 \leq K^*$ und wir können $K^*/(K^*)^2$ betrachten. $x^2 = d$ lösen entspricht der Untersuchung ob $d(K^*)^2 = (K^*)^2$. $\left|K^*/(K^*)^2\right|$ entspricht der Anzahl der Möglichkeiten in K^* kein Quadrat zu sein.

- Für $K = \mathbb{Z}/p\mathbb{Z}$:

$$\left(\mathbb{Z}/p\mathbb{Z}\right)/\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^*\right)^2 \cong \mathbb{Z}/2\mathbb{Z}$$

für $p \neq 2$,

$$\left(\mathbb{Z}/2\mathbb{Z}\right)/\left(\left(\mathbb{Z}/2\mathbb{Z}\right)^*\right)^2 \cong \{1\}.$$

- für $K = \mathbb{R}$:

$$R^*/(\mathbb{R}^*)^2 \cong \mathbb{Z}/2\mathbb{Z}.$$

$(x \in \mathbb{R}\colon\ \operatorname{sgn}(x)\sqrt{|x|^2}, -1 \notin (\mathbb{R}^*)^2)$

- Für $K = \mathbb{Q}$:

$$\mathbb{Q}^*/(\mathbb{Q}^*)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \bigoplus_{p\in\mathbb{P}} \mathbb{Z}/2\mathbb{Z}.$$

Beweis. Sei $\phi\colon \mathbb{Q}^* \to \mathbb{Z}/2\mathbb{Z} \times \bigoplus_{p\in\mathbb{P}} \mathbb{Z}/2\mathbb{Z}$, wobei $\mu(-1) = \bar{1}, \mu(+1) = \bar{0}$. Da jedes

$$x \mapsto (\mu(\operatorname{sgn}(x)), \nu_p(x) \pmod 2)$$

$x \in \mathbb{Q}^*$ höchstens endlich viele Primteiler in Zähler und Nenner besitzt, liegt das Bild von ϕ in der angegebenen Menge. ϕ ist Homomorphismus: wegen der bewiesenen Rechenregeln für $\nu_p(x)$. ϕ ist surjektiv ist klar. $\ker(\phi)$: $x = y^2 \implies x \in \ker\phi$. Ist $x \in \ker\phi$, so ist x positiv, für jede Primzahl p ist $\nu_p(x)$ gerade, also $x = \prod_{p\in\mathbb{P}} p^{2\nu} = \prod_{p\in\mathbb{P}} (p^\nu)^2 = (\prod_{p\in\mathbb{P}} p^\nu)^2$. Aus dem Homomorphiesatz folgt die Behauptung. □

Nun $K = \mathbb{Q}_p$. Wir definieren für $u \in \mathbb{Z}_p^*$:

$$\left(\frac{u}{p}\right) := \left(\frac{u \pmod p}{p}\right) = \left(\frac{x_0}{p}\right),$$

wenn $u = (x_0, x_1, \dots)$.

Satz 2.2.1:

Sei $x = p^n \cdot u \in \mathbb{Q}_p$ mit $u \in \mathbb{Z}_p^*$.

$$x \in (\mathbb{Q}_p^*)^2 \iff n \equiv 0 \pmod 2 \text{ und } \begin{cases} \left(\frac{u}{p}\right) & \text{für } p \neq 2 \\ u \equiv 1 \pmod 8 & \text{für } p = 2. \end{cases}$$

Beweis. Falls $x = y^2$, so gilt $\nu_p(x) = \nu_p(y^2) = 2\nu_p(y)$.

Ist n gerade, so ist $p^n u \in (\mathbb{Q}_p^*)^2 \iff u \in (\mathbb{Z}_p^*)^2$. Im Fall $p \neq 2$ folgt aus $u = v^2$: $\left(\frac{u}{p}\right) = \left(\frac{v^2}{p}\right) = \left(\frac{v}{p}\right)^2 = 1$. Umgekehrt, ist $\left(\frac{u}{p}\right) = 1$ so besitzt $f(x) = x^2 - u$ eine Nullstelle $\mod p$.

Für $f(y) \equiv 0 \pmod{p}$ ist $f'(y) = 2y \not\equiv 0 \pmod{p}$ und nach dem Theorem 2.1.17 von Hensel ($l = 0$) existiert ein $v \in \mathbb{Z}_p$ mit $f(v) = 0$. Im Fall $p = 2, u = v^2$ mit $v \in \mathbb{Z}_2^*$, sodass $2 \nmid u, 2 \nmid v$. $u = 1 + 2x, v = 1 + 2y$ mit $x, y \in \mathbb{Z}_2$. $1 + 2x = 1 + 4y + 4y^2 \implies x = 2y(1 + y)$. Es folgt $x \equiv 0 \pmod{4} \implies u \equiv 1 \pmod{8}$. Umgekehrt, sei $u \equiv 1 \pmod{8}$. 3 ist Nullstelle von $f(x) = x^2 - u \pmod{8}$ und $\nu_2(f'(3)) = \nu_2(6) = 1$ und aus Theorem 2.1.17 von Hensel ($l = 1$) folgt: $\exists x \in \mathbb{Z}_2 : f(x) = 0$, das heißt $u = x^2$. □

Korollar 2.2.2:

Sei $p \in \mathbb{P} \setminus \{2\}$. Dann ist

$$\phi : {}^{\mathbb{Q}_p^*}\!/_{(\mathbb{Q}_p^*)^2} \to {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \qquad (\text{, wobei } \mu(1) = 0, \mu(-1) = 1)$$
$$p^n u(\mathbb{Q}_p^*)^2 \mapsto \left(\mu\left(\left(\frac{u}{p}\right)\right), n \pmod 2\right)$$

ein Isomorphismus.

Beweis. Sei $\tilde{\phi} : \mathbb{Q}_p^* \to {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ analog definiert. $\tilde{\phi}$ ist Homomorphismus ✓
$\tilde{\phi}$ ist surjektiv: mit $\varepsilon \in \mathbb{Z}_p^*$ sodass $(\frac{\varepsilon}{p}) = -1$ ist $\tilde{\phi}(\varepsilon) = (1, 0), \tilde{\phi}(p) = (0, 1)$.
Aus dem Theorem 2.2.1 folgt $\ker \tilde{\phi} = (\mathbb{Q}_p^*)^2$, aus dem Homomorphiesatz folgt die Behauptung. □

Bemerkung 2.2.3:

$\{1, \varepsilon, p, \varepsilon p\}$ ist vollständiges Repräsentantensystem von ${}^{\mathbb{Q}_p^*}\!/_{(\mathbb{Q}_p^*)^2}$.

Korollar 2.2.4:

Für $p = 2$ ist

$$\phi : {}^{\mathbb{Q}_2^*}\!/_{(\mathbb{Q}_2^*)^2} \to \left({}^{\mathbb{Z}}\!/_{8\mathbb{Z}}\right)^* \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \cong \left({}^{\mathbb{Z}}\!/_{2\mathbb{Z}}\right)^3$$
$$2^n u(\mathbb{Q}_2^*)^2 \mapsto (u \pmod 8, n + 2\mathbb{Z})$$

ein Isomorphismus.

Bemerkung 2.2.5:

$\{\pm 1, \pm 5, \pm 2, \pm 10\}$ ist ein vollständiges Repräsentantensystem von ${}^{\mathbb{Q}_2^*}\!/_{(\mathbb{Q}_2^*)^2}$

Beispiel 2.2.6:
833 in $\mathbb{Q}_7$. $833 = 7^2 \cdot 17$. Berechne $(\frac{17}{7}) = (\frac{3}{7}) = -(\frac{7}{3}) = -1$, also ist 833 kein Quadrat in $\mathbb{Q}_7$.

Satz 2.2.7:
$x^2 = d$ hat genau dann eine rationale Lösung, wenn es Lösungen in $\mathbb{R}$ und $\mathbb{Q}_p$ $\forall p \in \mathbb{P}$ gibt.

Beweis. Jede rationale Lösung ist eine solche in $\mathbb{R}, \mathbb{Q}_p$.
Ist $x^2 = d$ in $\mathbb{R}$ lösbar, so ist $d > 0$ und ist $x^2 = d$ in $\mathbb{Q}_p$ lösbar, so ist $\nu_p(d)$ gerade. Also ist d ein Quadrat. □

Umformulierung: $dy^2 = z^2$ (setze $x = \frac{z}{y} \implies x^2 = d, x^2 = d \implies x^2 = d \cdot 1, x = z, y = 1$)
Verallgemeinerung: wir untersuchen die Lösbarkeit von $ax^2 + by^2 = z^2$ über $\mathbb{R}/\mathbb{Q}/\mathbb{Q}_p$.

Definition 2.2.8 (Hilbertsymbol):
Sei $p \in \mathbb{P} \cup \{\infty\}, a, b \in \mathbb{Q}_p^*$. Das Hilbertsymbol $(\frac{a,b}{p}) \in \{\pm 1\}$ genau dann gleich 1, wenn $ax^2 + by^2 = z^2$ eine Lösung $\neq (0,0,0)$ in $\mathbb{Q}_p^3$ besitzt.

Warum wird gerade $f(x,y,z) = ax^2 + by^2 - z^2$ untersucht?

Satz 2.2.9 (Trägheitssatz von Sylvester):
Sei $Q(x_1, \dots, x_n) = \sum_{i,j=1}^n a_{ij} x_i x_j$ mit $a_{ij} = a_{ji} \in K$ eine quadratische Form in n Variablen über K, wobei char $K \neq 2$. Dann existiert eine lineare Koordinatentransformation, die Q in $\tilde{Q} = \sum_{i=1}^n \alpha_i x_i^2$ überführt, mit $\alpha_i \neq 0$ für $i = 1, \dots, r$. r heißt dabei rang(Q).

Ist Q ternäre Form, so ist $Q \sim \alpha X^2 + \beta y^2 + \gamma z^2$. OBdA $\alpha, \beta, \gamma \neq 0$. Wir sind an der Darstellbarkeit von o interessiert.

$$\alpha x^2 + \beta y^2 = -\gamma z^2 \iff \underbrace{\frac{\alpha}{\gamma}}_{=:a} x^2 + \underbrace{\frac{\beta}{\gamma}}_{=:b} y^2 = z^2.$$

Lemma 2.2.10:

Für $a, b \in \mathbb{R}^*$

$$\left(\frac{a,b}{\infty}\right) = 1 \iff a > 0 \vee b > 0.$$

Beweis. ($\Longrightarrow$) weil $z^2 > 0 \implies a > 0 \vee b > 0$.
($\Longleftarrow$) ist oBdA $a > 0$, so ist $a \cdot 1^2 + b \cdot 0 = (\sqrt{a})^2$. □

Lemma 2.2.11:

Für $p \in \mathbb{P} \cup \{\infty\}$ gilt: (mit $a, b, c, d \in \mathbb{Q}_p^*$)

(1) $(\frac{a,b}{p}) = (\frac{b,a}{p})$
(2) $(\frac{a,1}{p}) = (\frac{a,-a}{p}) = 1$
(3) $(\frac{a,1-a}{p}) = 1$, falls $a \neq 1$
(4) $(\frac{a,b}{p}) = (\frac{ac^2,bd^2}{p})$
(5) $(\frac{ab,ac}{p}) = (\frac{ab,-bc}{p})$
(6) Falls $(\frac{a,c}{p}) = 1$, so gilt: $(\frac{a,b}{p}) = (\frac{a,bc}{p})$

Beweis. 1. ✓

2. $a \cdot 0^2 + 1 \cdot 1^2 = 1^2$, $a \cdot 1^2 - a \cdot 1^2 = 0^2$

3. $a \cdot 1^2 + (1-a) \cdot 1^2 = 1^2$

4. $ac^2x^2 + bd^2y^2 = z^2 \iff a(cx)^2 + b(dy)^2 = z^2$

5.

$$\begin{aligned} abx^2 + acy^2 = z^2 &\iff -z^2 + acy^2 = -abx^2 \\ &\iff \frac{1}{ab}z^2 - \frac{c}{b}y^2 = x^2 \end{aligned}$$

$$\begin{aligned} \implies \left(\frac{ab, ac}{p}\right) &= \left(\frac{\frac{1}{ab}, -\frac{c}{b}}{p}\right) \\ &\overset{2.2.11\,(4)}{=} \left(\frac{ab, -bc}{p}\right) \end{aligned}$$

6. Sei $(\frac{a,c}{p}) = (\frac{a,b}{p}) = 1$. $ax^2+cy^2 = z^2, a\tilde{x}^2+b\tilde{y}^2 = \tilde{z}^2$ Falls $y = 0$ oder $\tilde{y} = 0$, so gilt $ax^2+bcy^2 = z^2$ hat die Lösung $(x, 0, z)$ bzw. $(\tilde{x}, 0, \tilde{z})$. Falls $y, \tilde{y} \neq 0$, so ist $(x\tilde{z} + z\tilde{x}, y\tilde{y}, ax\tilde{x} + z\tilde{z})$ eine nicht-triviale Lösung von $ax^2 + bcy^2 = z^2$. $\implies (\frac{a,bc}{p}) = 1$.

   Umgekehrt: ist $(\frac{a,c}{p}) = (\frac{a,bc}{p}) = 1$, so folgt aus obiger Überlegung (ersetze b durch bc) $(\frac{a,bc}{p}) = (\frac{a,bcc}{p}) = (\frac{a,bc^2}{p}) = (\frac{a,b}{p})$. □

Satz 2.2.12:

Sei $p \in \mathbb{P} \setminus \{2\}$, $m, n \in \mathbb{Z}, u, v \in \mathbb{Z}_p^*$. Dann gilt:

(1) $(\frac{u,v}{p}) = 1$
(2) $(\frac{u,vp}{p}) = (\frac{u}{p})$
(3) $(\frac{up,vp}{p}) = (\frac{-uv}{p})$

Allgemein gilt:

$$\left(\frac{p^n u, p^m v}{p}\right) = (-1)^{mn\frac{p-1}{2}} \left(\frac{u}{p}\right)^m \left(\frac{v}{p}\right)^n \tag{2.3}$$

Beweis. 1. Untersuche $ux^2 + vy^2 = z^2$ und setzen $y = 1$. $ux^2 + v \equiv z^2 \pmod p$ hat stets eine Lösung $(\bar{x}, \bar{z}) \in (\mathbb{Z}/p\mathbb{Z})^2 \setminus \{\bar{0}, \bar{0}\}$.

   Sei $M_1 := \{u\bar{x}^2 + v \colon \bar{x} \in \mathbb{Z}/p\mathbb{Z}\}$, $M_2 := \{\bar{z}^2 \colon \bar{z} \in \mathbb{Z}/p\mathbb{Z}\}$. Es ist $|M_1| = |M_2| = \frac{p+1}{2}$. Daher gilt $M_1 \cap M_2 \neq \emptyset \implies \exists \bar{w} \in \mathbb{Z}/p\mathbb{Z} \colon u\bar{x}^2 + v = \bar{w} = \bar{z}^2$.

   Sei oBdA $\bar{x} \neq 0$. Wähle $z \in \mathbb{Z}_p$ mit $z \equiv \bar{z} \pmod p$ und betrachte das Polynom $f(x) = ux^2 + v - z^2$. Es ist nach Konstruktion $f(\bar{x}) = 0$ in $\mathbb{Z}/p\mathbb{Z}$. Weiters gilt $f'(\bar{x}) = 2\bar{x}u \not\equiv 0 \pmod p$. Nach dem Theorem 2.1.17 von Hensel existiert ein $x \in \mathbb{Z}_p$ mit $f(x) = 0$, das heißt $ux2 + v \cdot 1^2 = z^2$, also $(\frac{u,v}{p}) = 1$.

2. Angenommen $(\frac{u,vp}{p}) = 1$. Dann existiert Lösung (x, y, z) von $ux^2 + pvy^2 = z^2$. OBdA ist mindestens ein der 3 Komponenten in $\mathbb{Z}_p^*$. Behauptung: dann ist $x \in \mathbb{Z}_p^*$. Wäre nämlich $x \in p\mathbb{Z}_p^*$, so folge $z \in p\mathbb{Z}_p \implies y \in p\mathbb{Z}_p$, ein Widerspruch zur Annahme. $\mod p$ gilt: $0 \not\equiv ux^2 \equiv z^2 \pmod p \implies z \in \mathbb{Z}_p^*$ und es gilt: $u \equiv (\frac{z}{x})^2 \pmod p \implies (\frac{u}{p}) = 1$.

   Umgekehrt, sei $(\frac{u}{p}) = 1$. Dann ist $u \equiv \bar{z}^2 \pmod p$ lösbar. Mittels Theorem 2.1.17 folgt $z^2 = u$ hat Lösung $z \in \mathbb{Z}_p^*$. Dann gilt: $u \cdot 1^2 + pv \cdot 0^2 = z^2$ und somit $(\frac{u,pv}{p}) = 1$.

3.

$$\left(\frac{pu, pv}{p}\right) \overset{2.2.11\,(5)}{=} \left(\frac{pu, -uv}{p}\right) \overset{2.2.12\,(2)}{=} \left(\frac{-uv}{p}\right).$$

□

Satz 2.2.13:

Für $u2^n, v2^m$ mit $u, v \in \mathbb{Z}_2^*$ gilt:

$$\left(\frac{u2^n, v2^m}{2}\right) = (-1)^{\frac{u-1}{2}\cdot\frac{v-1}{2}} (-1)^{n\frac{v^2-1}{8}} (-1)^{m\frac{u^2-1}{8}}. \tag{2.4}$$

Für das Repräsentantensystem $\{\pm 1, \pm 5, \pm 2, \pm 10\}$ von $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ gilt:

	1	−1	5	−5	2	−2	10	−10
1	+1	+1	+1	+1	+1	+1	+1	+1
−1	+1	−1	+1	−1	+1	−1	+1	−1
5	+1	+1	+1	+1	−1	−1	−1	−1
−5	+1	−1	+1	−1	−1	+1	−1	+1
2	+1	+1	−1	−1	+1	+1	−1	−1
−2	+1	−1	−1	+1	+1	−1	−1	+1
10	+1	+1	−1	−1	−1	−1	+1	+1
−10	+1	−1	−1	+1	−1	+1	+1	−1

Beweis. Tabelle nachprüfen.

2. Zeile:

- $(\frac{-1,2}{2})$: $-1\cdot 1^2 + 2\cdot 1^2 = 1^2$,
- $(\frac{-1,5}{2})$: $-1\cdot 1^2 + 5\cdot 1^2 = 2^2$,
- $(\frac{-1,10}{2})$: $-1\cdot 1^2 + 10\cdot 1^2 = 3^2$.
- $(\frac{-1,-2}{2})$: $-x^2 - 2y^2 = z^2$. OBdA.: $x, z \in \mathbb{Z}_2^* \implies x^2 \equiv z^2 \equiv 1 \pmod 8 \implies -2y^2 \equiv 2 \pmod 8 \implies y^2 \equiv 1 \pmod 4$ ↯, also $(\frac{-1,-2}{2}) = -1$.
- $(\frac{-1,-1}{2}) \overset{2.2.11\,(4)}{=} (\frac{-1,-4}{2}) = (\frac{-1,-2\cdot 2}{2}) \overset{2.2.11\,(6)}{=} (\frac{-1,-2}{2}) = -1$.
- $(\frac{-1,-5}{2}) = (\frac{-1,-1\cdot 5}{2}) \overset{2.2.11\,(6)}{=} (\frac{-1,-1}{2}) = -1$.
- $(\frac{-1,-10}{2}) = (\frac{-1,-1\cdot 10}{2}) \overset{2.2.11\,(6)}{=} (\frac{-1,-1}{2}) = -1$.

Aus Punkt 2.2.11 (2) folgt: $(\frac{5,-5}{2}) = (\frac{2,-2}{2}) = (\frac{10,-10}{2}) = +1$.
Es gilt: $-5(\mathbb{Q}_2^*)^2 = 3(\mathbb{Q}_2^*)^2 = 11(\mathbb{Q}_2^*)^2$, sodass nach Punkt 2.2.11 (3)

$$\left(\frac{-5,-2}{2}\right) = \left(\frac{3,-2}{2}\right) = 1,$$
$$\left(\frac{-5,-10}{2}\right) = \left(\frac{11,-10}{2}\right) = 1.$$

Nach Punkt 2.2.11 (5): $(\frac{-2,-10}{2}) = (\frac{-2\cdot 1,-2\cdot 5}{2}) = (\frac{-2,-5}{2}) = +1$

Die anderen Symbole ergeben sich mittels Punkt 2.2.11 (6), da sich die entsprechenden a, b in $(\frac{a,b}{2})$ lediglich in einem Vorzeichen unterscheiden. Beispiel dazu: $(\frac{5,5}{2}) = (\frac{5,-1\cdot -5}{2}) = (\frac{5,-1}{2}) = +1$.□

Korollar 2.2.14:

Das Hilbertsymbol ist bimultiplikativ.

$$\left(\frac{a,b}{p}\right)\cdot\left(\frac{a,c}{p}\right) = \left(\frac{a,bc}{p}\right)$$
$$\left(\frac{a,c}{p}\right)\cdot\left(\frac{b,c}{p}\right) = \left(\frac{ab,c}{p}\right)$$

Beweis. Für $p \in \mathbb{P}$ folgt das aus den angegebenen geschlossenen Ausdrücken Gleichungen (2.3) und (2.4), denn $u \mapsto (\frac{u}{p}), u \mapsto (-1)^{\frac{u-1}{2}} \pmod 2, u \mapsto (-1)^{\frac{u^2-1}{8}} \pmod 2$ sind multiplikativ und das Produkt multiplikativer Funktionen ist ist wieder multiplikativ.

Für $p = \infty$:

$$\left(\frac{-1,-1}{\infty}\right)\cdot\left(\frac{-1,-1}{\infty}\right) = (-1)\cdot(-1) = 1 = \left(\frac{-1,1}{\infty}\right) = \left(\frac{-1,(-1)\cdot(-1)}{\infty}\right),$$

alle anderen Fälle folgen. □

Satz 2.2.15 (Produktformel):

Für $a, b \in \mathbb{Q}^*$ gilt:

$$\prod_{p\in\mathbb{P}\cup\{\infty\}} \left(\frac{a,b}{p}\right) = 1.$$

Beweis. OBdA seien $a, b \in \mathbb{Z}$ (denn $(\frac{a,b}{p})$) hängt nur von der Quadratrestklasse von a und b ab, multiplizieren mit Quadraten der Nenner.

Nur endlich viele Hilbertsymbole im Produkt sind $\neq 1$, denn für $p \in \mathbb{P} \setminus \{2\}$ und $p \nmid a, p \nmid b$ ist $(\frac{a,b}{p}) = 1$. Wegen der Bimultiplikativität und wegen $(\frac{1,a}{p}) = 1$ genügt es, folgende Fälle zu betrachten: (mit $r \neq q \in \mathbb{P} \setminus \{2\}$)

$$(a,b) = (-1,-1), (-1,2), (-1,q), (2,2), (2,q)(q,q), (q,r).$$

Beachte, dass

$$(\frac{2,2}{p}) = (\frac{2\cdot 1, 2\cdot 1}{p}) \overset{2.2.11\,(5)}{=} (\frac{2,-1}{p})$$
$$(\frac{q,q}{p}) = (\frac{q\cdot 1, q\cdot 1}{p}) \overset{2.2.11\,(5)}{=} (\frac{q,-1}{p}).$$

Für diese 5 Fälle gilt folgende Tabelle:

(a,b)	$(\frac{a,b}{\infty})$	$(\frac{a,b}{2})$	$(\frac{a,b}{2})$	$(\frac{a,b}{r})$	$\prod$
$(-1,-1)$	-1	-1	$+1$	$+1$	1
$(-1,2)$	$+1$	$+1$	$+1$	$+1$	1
$(-1,q)$	$+1$	$(-1)^{\frac{q-1}{2}}$	$(\frac{-1}{q})$	$+1$	1 (wegen 1. Ergänzungssatz[1])
$(2,q)$	$+1$	$(-1)^{\frac{q^2-1}{8}}$	$(\frac{2}{q})$	$+1$	1 (wegen 2. Ergänzungssatz[2])
(r,q)	$+1$	$(-1)^{\frac{q-1}{2}\cdot\frac{r-1}{2}}$	$(\frac{r}{q})$	$(\frac{q}{r})$	1 (wegen QRG[3])

□

Korollar 2.2.16:

Die Gleichung $ax^2 + by^2 = z^2$ habe Lösungen in $\mathbb{R}$ und in $\mathbb{Q}_p (p \in \mathbb{P} \setminus \{q\})$. Dann hat sie auch eine in $\mathbb{Q}_q$.

Satz 2.2.17 (Minkowski-Hasse ($n = 3$)):

Seien $a, b \in \mathbb{Q}^*$. Die Gleichung $ax^2 + by^2 = z^2$ hat genau dann eine nicht-triviale Lösung in $\mathbb{Q}$, wenn sie nicht-triviale Lösungen in $\mathbb{R}$ und in allen $\mathbb{Q}_p, p \in \mathbb{P}$ besitzt.

Beweis. Jede rationale Lösung ist eine solche in $\mathbb{R}, \mathbb{Q}_p, p \in \mathbb{P}$.

Umgekehrt, seien oBdA a, b quadratfrei und $|a| \leq |b|$. Wir zeigen die Behauptung durch Induktion nach $n := |a| + |b|$. Induktionsanfang bei $n = 2$. Es sind nur die Fälle $x^2 - y^2 = z^2$, $x^2 + y^2 = z^2$, $-x^2 - y^2 = z^2$ zu betrachten. In den ersten beiden Fällen ist $(1, 0, 1)$ Lösung, im dritten Fall gibt es keine reelle Lösung.

Induktionsschritt: $n \geq 3 \implies |b| \geq 2, b \neq \pm 1$. Behauptung: a ist ein Quadrat $\mod b$. Sei $\mathbb{P} \ni p \mid b$ und (x, y, z) eine nicht-triviale Lösung von $ax^2 + by^2 = z^2$ über $\mathbb{Q}_p$. Wir dürfen wieder voraussetzen, dass $x, y, z \in \mathbb{Z}_p$ und $x, z \in \mathbb{Z}_p^*$. Daher ist $ax^2 \equiv z^2 \pmod p$, also $a \equiv (\frac{z}{x})^2 \pmod p$. b ist quadratfrei $\implies b = \prod_{i=1}^{s} p_i$ mit $p_i \neq p_j$ für $i \neq j$. Nach dem CRS ist $\mathbb{Z}/b\mathbb{Z} \cong \prod_{i=1}^{s} \mathbb{Z}/p_i\mathbb{Z}$. In jedem $\mathbb{Z}/p_i\mathbb{Z}$ ist a ein Quadrat, daher auch in $\mathbb{Z}/b\mathbb{Z}$. Folglich existieren $t, b' \in \mathbb{Z}$ mit $a + bb' = t^2$ und wir können annehmen, dass $|t| \leq \frac{b}{2}$. Falls $b' = 0$, also $t^2 = a$, so ist $(1, 0, t)$ die gesuchte Lösung. Ansonsten gilt $b' = b'' \cdot c^2$ mit b'' quadratfrei. Dann gilt: $a \cdot 1^2 + bb'' \cdot c^2 = t^2$, also $(\frac{a,bb''}{p}) = 1 \forall p \in \mathbb{P} \cup \{\infty\}$. Nach Voraussetzung gilt $(\frac{a,b}{p}) = 1$. Nach Punkt 2.2.11 (6) folgt $(\frac{a,b''}{p}) = (\frac{a,bb''}{p}) = 1$.

$$|b''| \leq |b'| = \left|\frac{t^2 - a}{b}\right| \leq \frac{t^2}{|b|} + \frac{|a|}{|b|} \leq \frac{|b|}{4} + 1 < |b|\,.$$

[1] Leonhard Summerer. *Algebra*. 2022. URL: https://anton.mosich.at/Algebra.pdf, Korollar 4.4.13.
[2] Leonhard Summerer. *Algebra*. 2022. URL: https://anton.mosich.at/Algebra.pdf, Korollar 4.4.15.
[3] Leonhard Summerer. *Algebra*. 2022. URL: https://anton.mosich.at/Algebra.pdf, Satz 4.4.16.

$\Longrightarrow$ nach Induktionsvoraussetzung: $\exists \tilde{x}, \tilde{y}, \tilde{z} \neq (0,0,0)\colon a\tilde{x}^2 + b''\tilde{y}^2 = \tilde{z}^2$. Falls $\tilde{y} = 0$, dann ist $(\tilde{x}, 0, \tilde{z}) \in \mathbb{Q}^3$ die gesuchte Lösung. Ansonsten:

$$\begin{cases} a\tilde{x}^2 + b''\tilde{y}^2 = \tilde{z}^2 \\ a \cdot 1^2 + bb''c^2 = t^2 \end{cases} \quad \Longrightarrow (t\tilde{x} + \tilde{z}, c\tilde{y}, a\tilde{x} + t\tilde{z}) \text{ Lösung von } ax^2 + bb''^2y^2 = z^2.$$

$$\begin{aligned} a(t\tilde{x} + \tilde{z})^2 + bb''^2c^2\tilde{y}^2 &\overset{!}{=} (a\tilde{x} + t\tilde{z})^2 \\ at^2\tilde{x}^2 + a\tilde{z}^2 + \cancel{2at\tilde{x}\tilde{z}} + bb''^2c^2\tilde{y}^2 &= a^2\tilde{x}^2 + t^2\tilde{z}^2 + \cancel{2at\tilde{x}\tilde{z}} \\ a(\cancel{a} + bb''c^2)\tilde{x}^2 + \cancel{a\tilde{z}^2} + bb''^2c^2\tilde{y}^2 &= \cancel{a^2\tilde{x}^2} + (\cancel{a} + bb''c^2)\tilde{z}^2 \\ abb''c^2\tilde{x}^2 + bb''^2c^2\tilde{y}^2 &= bb''c^2\tilde{z}^2 \\ \cancel{bb''c^2}(a\tilde{x}^2 + b''\tilde{y}^2) &= \cancel{bb''c^2}\tilde{z}^2 \end{aligned}$$

□

Beispiel 2.2.18:

Zeige, dass $\frac{1}{8}x^2 + \frac{23}{9}y^2 = z^2$ eine rationale Lösung besitzt. $\Longleftrightarrow$ $2x^2 + 23y^2 = z^2$ hat rationale Lösung. $\Longleftrightarrow$ $(\frac{2,23}{p}) = 1\ \forall p \in \mathbb{P} \cup \{\infty\}$ Es ist klar, dass $(\frac{2,23}{p}) = 1 \forall p \in (\mathbb{P} \cup \{\infty\}) \setminus \{2, 23\}$.

$$\left(\frac{2,23}{23}\right) = \left(\frac{2}{23}\right) \overset{\text{2. ES}}{=} 1, \qquad \left(\frac{2,23}{2}\right) = \left(\frac{2,-1}{2}\right) = 1$$

Die zweite der Rechnungen ist eigentlich nicht nötig, wegen Theorem 2.2.15

2.3 Quadratische Formen und der allgemeine Satz von Minkowski-Hasse

Definition 2.3.1:

V sei ein Vektorraum über dem Körper $\mathbb{K}$ mit $\operatorname{char}\mathbb{K} \neq 2$. Eine quadratische Form Q ist eine Abbildung $Q\colon V \to \mathbb{K}$ mit

1. $Q(aX) = a^2Q(X) \forall a \in \mathbb{K}, x \in V$.
2. $(x, y) \mapsto \frac{1}{2}(Q(x + y) - Q(x) - Q(y))$ ist bilinear.

Ist $(b_i)_{i=1}^n$ eine Basis von V über $\mathbb{K}$, so ist $(a_{ij}) =: A$ die Darstellungsmatrix von Q bezüglich $(b_i)_{i=1}^n$ gegeben durch $a_{ij} = \frac{1}{2}(Q(b_i + b_j) - Q(b_i) - Q(b_j))$. $f_Q(x) = \sum_{i,j} a_{ij}x_ix_j = x^tAx$.

Wegen des Trägheitssatzes von Sylvester (2.2.9) existiert eine Basis mit

$$f_Q(x) = \sum_{i=1}^{r} a_i x_i^2, a_i \in \mathbb{K}.$$

Für $\operatorname{rg} Q = n$ gilt $r = n$.

Definition 2.3.2:

Q sei eine quadratische Form über $\mathbb{K}$ vom Rang r in r Variablen. $b \in \mathbb{K}$ wird von Q dargestellt genau dann wenn $\exists x \neq 0 \in \mathbb{K}^r \colon Q(x) = b$.

Q heißt isotrop, falls 0 von Q dargestellt wird. Ansonsten wird Q anisotrop genannt.

Bemerkung 2.3.3:

- Darstellbarkeit von b beziehungsweise die Isotropie von Q hängt lediglich von den Restklassen der a_i beziehungsweise von b in ${}^{\mathbb{K}^*}\!/_{(\mathbb{K}^*)^2}$ ab.
- Q ist genau dann über $\mathbb{R}$ isotrop, wenn nicht alle a_i das selbe Vorzeichen haben.

Satz 2.3.4:

Sei Q über $\mathbb{K}$ isotrop. Dann stellt Q jedes $b \in \mathbb{K}$ dar. (char $\mathbb{K} \neq 2$ ist hier wichtig)

Beweis. Sei $Q(x) = \sum_{i=1}^{r} a_i x_i^2$ isotrop, das heißt $\exists (x_1, \ldots, x_r) \colon Q(x_1, \ldots, x_r) = 0$. OBdA sei $x_1 \neq 0$. Für $\lambda \in \mathbb{K}^*$ setzen wir

$$\begin{aligned} y_1 &= x_1(1+\lambda) \\ y_i &= x_i(1-\lambda) \; i = 2, \ldots, r. \end{aligned}$$

$$\begin{aligned} \sum_{i=1}^{r} a_i y_i^2 &= a_1 x_1^2 (1+\lambda)^2 - a_1 x_1^2 (1-\lambda)^2 + \sum_{i=1}^{r} a_i x_i^2 (1-\lambda)^2 \\ &= a_1 x_1^2 \underbrace{\left((1+\lambda)^2 - (1-\lambda)^2\right)}_{4\lambda} + (1-\lambda)^2 + \underbrace{\sum_{i=1}^{r} a_i x_i^2}_{=0 \text{ nach Voraussetzung}} \end{aligned}$$

Wähle nun $\lambda := \frac{b}{4 a_1 x_1^2}$, sodass $Q(y_1, \ldots, y_r) = b$. □

Lemma 2.3.5:

Jede isotrope quadratische Form $Q = \sum a_i x_i^2$ über $\mathbb{K}$ mit $|\mathbb{K}| \geq 6$ besitzt eine Nullstelle $(x_1, \ldots, x_r)$ mit $x_i \neq 0 \forall i = 1, \ldots, r$.

Beweis. Q isotrop $\implies \exists y = (y_1, \ldots, y_r)$ mit $Q(y_1, \ldots, y_r) = 0, y \neq 0$.
OBdA.: $y_1, \ldots, y_n \neq 0, y_{n+1}, \ldots, y_r = 0$ für ein $n \in \{1, \ldots, r\}$. Falls $n < r$:

$$\exists x = (x_1, \ldots, x_r) \colon x_1, \ldots, x_{n+1} \neq 0 \wedge Q(x) = 0.$$

Wähle $x_i = y_i$ für $i = 1, \ldots, n-1, n+2, \ldots, r$ und bestimme $x_n, x_{n+1} \neq 0$ mit $a_n x_n^2 + a_{n+1} x_{n+1}^2 = a_n y_n^2 + \overbrace{a_{n+1} y_{n+1}^2}^{=0}$ folgendermaßen. Aus $\frac{(1-\lambda)^2}{(1+\lambda)^2} + \frac{4\lambda}{(1+\lambda)^2} = 1$ folgt:

$$\begin{aligned} a_n y_n^2 &= a_n \left(\frac{(1-\lambda) y_n}{1+\lambda} \right)^2 + a_n \lambda \left(\frac{2 y_n}{1+\lambda} \right)^2 \\ &= a_n \left(\frac{(1-\lambda) y_n}{1+\lambda} \right)^2 + a_{n+1} \frac{a_n \lambda}{a_{n+1}} \left(\frac{2 y_n}{1+\lambda} \right)^2 \end{aligned}$$

Wähle nun $\lambda = \mu^2 \frac{a_{n+1}}{a_n}$, wobei $\mu \in \mathbb{K}$ mit $\mu \neq 0, \mu^2 \neq \pm \frac{a_n}{a_{n+1}}$. Solch ein μ existiert, da $|\mathbb{K}| \geq 6$. Die Wahl von μ garantiert, dass $\lambda \neq \pm 1$. Mit $x_n = \frac{(1-\lambda) y_n}{1+\lambda}$ und $x_{n+1} = \frac{2\mu y_n}{1+\lambda} \neq 0$ folgt:

$$a_n x_n^2 + a_{n+1} x_{n+1}^2 = a_n y_n^2$$

und $Q(x_1, \ldots, x_r) = Q(y_1, \ldots, y_r) = 0$, wobei $x_1, \ldots, x_{n+1} \neq 0$. □

Angenommen wir wollen $x_r = 1$. Dann $\exists y_1, \ldots, y_r$ mit $y_r \neq 0 \colon Q(y_1, \ldots, y_r) = 0$. Dann ist $Q(\frac{y_1}{y_r}, \frac{y_2}{y_r}, \ldots, 1) = 0$.
Nun untersuchen wir die Isotropie von Formen über $\mathbb{Q}_p$.

Lemma 2.3.6:

Sei $p \neq 2$ prim, $Q = \sum_{i=1}^r a_i x_i^2$ mit $a_i \in \mathbb{Q}_p$. Falls $r \geq 3$ und $a_1, a_2, a_3 \in \mathbb{Z}_p^*$, so ist Q isotrop.

Beweis. $\tilde{Q}(x) = a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2$ erfüllt $\tilde{Q}(x) = 0$ genau dann wenn

$$\frac{a_1}{-a_3} x_1^2 + \frac{a_2}{-a_3} x_2^2 = x_3^2.$$

Diese Gleichung besitzt genau dann eine nicht-triviale Lösung, wenn $\left(\frac{\frac{-a_1}{a_3}, \frac{-a_2}{a_3}}{p} \right) = 1$. Dies folgt aus $\frac{-a_1}{a_3}, \frac{-a_2}{a_3} \in \mathbb{Z}_p^*$. $\tilde{Q}$ ist isotrop $\implies$ Q ist isotrop. □

Satz 2.3.7:
Für $p \in \mathbb{P}$ ist jede quadratische Form vom Rang ≥ 5 über $\mathbb{Q}_p$ isotrop.

Beweis. Sei $Q = \sum_{i=1}^{r} a_i x_i^2$ mit $r \geq 5, a_i \in \mathbb{Q}_p$. Da die Isotropie von Q nur von den Quadratrestklassen der a_i abhängt, kann oBdA $a_i \in \mathbb{Z}_p$ quadratfrei vorausgesetzt werden. Durch, falls notwendig, Multiplikation mit p kann erreicht werden, dass mindestens 3 a_i in $\mathbb{Z}_p^*$ liegen.

$$Q = u_1 x_1^2 + u_2 x_2^2 + u_3 x_3^2 + \cdots + u_s x_s^2 + p(u_{s+1} x_{s+1}^2 + \cdots + u_r x_r^2)$$

mit $u_i \in \mathbb{Z}_p^*$ und $s \geq 3$. Für $p \neq 2$ folgt aus dem Theorem 2.3.6 unmittelbar die Isotropie von Q.
Für $p = 2$ zeigen wir die Existenz einer Nullstelle $\mod 8$.

1. Fall $s \leq 4 < 4$: Wir konstruieren $(\tilde{x}_1, x_2, \ldots, x_r)$ mit $Q(\tilde{x}_1, x_2, \ldots, x_r) \equiv 0 \pmod 8$. $\tilde{x}_1 = x_2 := 1, x_4 = \cdots = x_{r-1} = 0$. Aus $u_i \in \mathbb{Z}_2^*$ folgt $u_i \equiv 1 \pmod 2$. Daher ist $u_1 + u_2 \equiv 0 \pmod 2$. Wähle $x_r := \frac{u_1+u_2}{2} \in \mathbb{Z}_2$. Setze $x_3 := x_r + u_r x_r^2$. Wegen $x_r \equiv x_r^2$ und $u_r \equiv 1 \pmod 2$ folgt $x_3 \in 2\mathbb{Z}_2$.

$$\begin{aligned} Q(\tilde{x}_1, x_2, \ldots, x_r) &= u_1 \tilde{x}_1^2 + u_2 x_2^2 + u_3 x_3^2 + 2u_r x_r^2 \\ &= 2x_r + 2u_r x_r^2 + u_3 x_3^2 \\ &= 2x_3 + u_3 x_3^2 = x_3(2 + u_3 x_3) \end{aligned}$$

Falls $x_3 \equiv 0 \pmod 4$, so ist $x_3(2 + u_3 x_3) \equiv 0 \pmod 8$, da $x_3 \equiv 0 \pmod 2$. Falls $x_3 \equiv 2 \pmod 4$, so ist $x_3 = 2 + 4x_3'$ und daher

$$x_3(2 + u_3 x_3) = (2 + 4x_3')(2 + u_3(2 + 4x_3')) \equiv 4 + 4u_3 \pmod 8 \equiv 0 \pmod 8.$$

2. Fall $s \geq 5$. OBdA gilt $u_i \in \{\pm 1, \pm 5\}$ sodass $u_1 \equiv \pm 1 \pmod 4$. $\implies \exists \tilde{x}_1, x_2, x_3, x_4 \in \{0, 1\}$, nicht alle gleich 0, mit $u_1 \tilde{x}_1^2 + u_2 x_2^2 + u_3 x_3^2 + u_4 x_4^2 \equiv 0 \pmod 4$. OBdA $\tilde{x}_1 = 1$. Setze $b := \frac{1}{4}(u_1 \tilde{x}_1^2 + u_2 x_2^2 + u_3 x_3^2 + u_4 x_4^2) \in \mathbb{Z}_2$ und $x_5 := 2b$. Dann ist $u_1 \tilde{x}_1^2 + u_2 x_2^2 + u_3 x_3^2 + u_4 x_4^2 + u_5 x_5^2 = 4b + 4b^2 u_4 = 4b(1 + bu_5)$ und für $b \equiv 0 \pmod 2$ ist $4b \equiv 0 \pmod 8$, für $b \equiv 1 \pmod 2$ ist $1 + u_5 b \equiv 0 \pmod 2$. $\tilde{x}_1, x_2, \ldots x_r$ sei Nullstelle von $Q \mod 8$ mit $\tilde{x}_1 = 1$. Setze $c := \frac{-1}{u_1}(\sum_{i=2}^{r} a_i x_i^2)$. Dann ist $c \equiv \tilde{x}_1^2 \equiv 1 \pmod 8$. Somit existiert die Wurzel von c in $\mathbb{Q}_2$, wir nennen sie x_1. Dann ist $Q(x_1, \ldots, x_r) = 0$. □

Korollar 2.3.8:
Jede quadratische Form vom Rang 4 über $\mathbb{Q}_p$ stellt jedes $b \in \mathbb{Q}_p^*$ dar.

Beweis. Sei $Q = \sum_{i=1}^{4} a_i x_i^2, b \in \mathbb{Q}_p^*$. Betrachte die Form $Q - bx_5^2$. Sie ist nach Theorem 2.3.7 isotrop und hat nach Theorem 2.3.5 sogar eine Nullstelle für die $x_5 \neq 0$, da $\left|\mathbb{Q}_p\right| = \infty$.

$$Q\left(\frac{x_1}{x_5}, \frac{x_2}{x_5}, \ldots, \frac{x_4}{x_5}\right) = b.$$

□

Satz 2.3.9 (Minkowski-Hasse für allgemeine quadratische Formen):
Eine quadratische Form ist genau dann isotrop über $\mathbb{Q}$, wenn sie es über $\mathbb{R}$ und $\mathbb{Q}_p, p \in \mathbb{P}$ ist.

Beweis. Jede globale Nullstelle ist auch lokale Nullstelle.
Umgekehrt, sei Q isotrop über $\mathbb{R}$ und über $\mathbb{Q}_p, p \in \mathbb{P}$. OBdA $Q = \sum_{i=1}^{r} a_i x_i^2, a_i \neq 0$.

$r = 1$: $Q = ax^2$ hat über keinem der Körper eine nicht-triviale Nullstelle.

$r = 2$: kann immer auf $ax^2 = y^2 \iff a = (\frac{y}{x})^2$ zurückgeführt werden wofür die Aussage schon gezeigt ist.

$r = 3$: kann immer auf $ax^2 + by^2 = z^2$ zurückgeführt werden, wofür die Aussage in Theorem 2.2.17 schon gezeigt ist.

$r \geq 4$: Zeige die Behauptung durch Induktion nach r. Q isotrop über $\mathbb{R} \implies$ oBdA $a_1 > 0, a_3 < 0$. Betrachte nun die Formen $f = a_1x_1^2 + a_2x_2^2, g = -a_3x_3^2 - a_4x_4^2 - \cdots - a_rx_r^2$. Q isotrop über $\mathbb{R} \implies$ oBdA $a_1 > 0, a_3 < 0$. Betrachte nun die Formen $f = a_1x_1^2 + a_2x_2^2, g = -a_3x_3^2 - a_4x_4^2 - \cdots - a_rx_r^2$. $\rightarrow$ gesucht ist ein $b \in \mathbb{Q}$ mit $b = f(x_1, x_2), b = g(x_3, \ldots, x_r)$ nicht-trivial $\implies Q(x_1, \ldots, x_r) = f(x_1, x_2) - g(x_3, \ldots, x_r) = b - b = 0$. Sei $P := \{p \in \mathbb{P} : p \mid a_i \text{ für ein } 1 \leq i \leq r\} \cup \{2\}$. Für $p \in P$: $\exists (y_1, \ldots, y_r) \in \mathbb{Q}_p^r$ mit $Q(y) = 0$ und definieren $b_p := f(y_1, y_2) = a_1y_1^2 + a_2y_2^2 = -a_3y_3^2 - \cdots - a_ry_r^2 = g(y_3, \ldots, y_r)$ und wir dürfen annehmen, dass $(y_1, y_2), (y_3, \ldots, y_r) \neq 0$. Falls $b_p = 0$, so sind f, g isotrop und stellen daher alle Elemente von $\mathbb{Q}_p^*$ dar, also auch z.B. $b_p = 1$. Wir können also immer $b_p \neq 0$ voraussetzen. OBdA ist $b_p \in \mathbb{Z}_p \setminus p^2\mathbb{Z}_p$. Mittels CRS erhalten wir eine Lösung b von $\begin{cases} x \equiv b_2 \pmod{16} \\ x \equiv b_p \pmod{p^2} \quad \text{für } p \in P \setminus \{2\} \end{cases}$ die eindeutig bestimmt ist $\mod 4 \prod_{p \in P} p^2 =: m$.
Wir wählen $b > 0$ und definieren

$$F := -by^2 + f, \; G := -by^2 + g.$$

Falls F, G isotrop über $\mathbb{Q}$ sind, so gibt es Nullstellen (y, x_1, x_2) von F, $(z, x_3, \ldots, x_r)$ von G mit $y = z = 1$, sodass wie gewünscht $f(x_1, x_2) = b$, $g(x_3, \ldots, x_r) = b$. Da F, G Rang $< r$ haben, genügt es nach Induktionsvoraussetzung zu zeigen, dass sie isotrop über $\mathbb{R}$ und $\mathbb{Q}_p, p \in \mathbb{P}$ sind.

- Über $\mathbb{R}$: $-b < 0, a_1 > 0, -b < 0, -a_3 > 0 \implies F, G$ isotrop über $\mathbb{R}$.
- Über $\mathbb{Q}_p$: sei zunächst $p \in P$. Da $b_p \in \mathbb{Z}_p \setminus p^2\mathbb{Z}_p$ folgt $\begin{cases} b_2b^{-1} \equiv 1 \pmod{8} \\ b_pb^{-1} \equiv 1 \pmod{p^2} \end{cases}$. Es folgt: b_pb^{-1} sind Quadrate in $\mathbb{Q}_p^* \implies$

$$\begin{cases} -b\left(\sqrt{b_pb^{-1}}\right)^2 + f(y_1, y_2) = -b_p + f(y_1, y_2) = 0 \\ -b\left(\sqrt{b_pb^{-1}}\right)^2 + g(y_3, \ldots, y_r) = -b_p + g(y_3, \ldots, y_r) = 0 \end{cases} \overset{\text{IV}}{\implies} F, G$$

sind isotrop über $\mathbb{Q}_p$ nach Induktionsvoraussetzung.

Sei nun $p \in \mathbb{P} \setminus P$. Falls $p \nmid b$, so sind alle Koeffizienten von F und G aus $\mathbb{Z}_p^*$ und daher isotrop über $\mathbb{Q}_p$ (da Rang von $F, G \geq 3$).

Einziges verbleibendes Problem sind diejenigen $p \in \mathbb{P}$ mit $p \notin P, p \mid b$. (Falls $r \geq 5$, so ist $\operatorname{rang}(g) \geq 3$ und somit g und a fortiori G isotrop.) b war $\mod m$ eindeutig bestimmt, wir wollen daher versuchen, ein b zu finden, das nur einen Primfaktor hat, der nicht in P liegt. Dazu sei $d := \operatorname{ggT}(b, m)$. Dann sind $\frac{b}{d}$ und $\frac{m}{d}$ teilerfremd $\overset{\text{Theorem 3.5.6}}{\Longrightarrow} \exists k\colon \frac{b}{d} + k\frac{m}{d} = q \in \mathbb{P} \implies da = b + km$. Wir ersetzen nun b im Beweis durch dq. Es folgt aus der Produktformel (2.2.15), dass $\frac{1}{b}F = -y^2 + \frac{a_1}{b}x_1^2 + \frac{a_2}{b}x_2^2$ isotrop über $\mathbb{R}$ und $\mathbb{Q}_p, p \neq q$ und daher über allen $\mathbb{Q}_p$.

Falls $r = 4$, so muss G analog behandelt werden, um die Isotropie über allen $\mathbb{Q}_p$ zu zeigen.

Aus der Induktionsvoraussetzung folgt die Isotropie von F und G über $\mathbb{Q}$, daraus folgt, dass f und g b simultan darstellen und der Beweis ist abgeschlossen. □

Theorem 2.3.9 wird auch Lokal-Global-Prinzip genannt.

Korollar 2.3.10:

Eine quadratische Form vom Rang ≥ 5 ist genau dann isotrop über $\mathbb{Q}$, wenn sie es über $\mathbb{R}$ ist.

Das Analogon zum Theorem 2.3.9 gilt nicht für Formen vom Grad ≥ 3.

Beispiel 2.3.11 (Selmer's Beispiel):

$3x^3 + 4y^3 + 5z^3 = 0$ hat über $\mathbb{Q}$ nur die triviale Lösung, aber nicht-triviale Lösungen über $\mathbb{R}$ und $\mathbb{Q}_p (p \in \mathbb{P})$.

- über $\mathbb{R}$: ist klar
- über $\mathbb{Q}_p$: Wir fangen an mit dem Fall $p = 3$. Setze $x = 0, z = -1$, sodass $4y^3 - 5 = 0$ zu lösen bleibt. $f(2) = 27 \equiv 0 \pmod{3^3}, f'(2) = 48 \equiv 0 \pmod 3, \not\equiv 0 \pmod 9$. Aus Theorem 2.1.17 folgt: $\exists y \in \mathbb{Q}_3$ mit $f(y) = 0$.

  Nun der Fall $p = 5$: setze $x = 1, z = 0$, sodass $g(y) = 4y^3 + 3 = 0$ zu lösen ist. $g(2) = 35 \equiv 0 \pmod 5, g'(2) = 48 \not\equiv \pmod 5$. Mittels Theorem 2.1.17 folgt: $\exists y \in \mathbb{Q}_5$ mit $g(y) = 0$.

  Sei $p \in \mathbb{P} \setminus \{3, 5\}$. $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ ist eine zyklische Gruppe der Ordnung $p - 1$.

  - Falls $p - 1 \equiv 0 \pmod 3 \iff p \equiv 1 \pmod 3$, so bilden die Kuben eine Untergruppe vom Index 3.

- Falls $p \not\equiv 1 \pmod 3$, so folgt aus $\text{ggT}(p-1,3) = 1$, dass jedes Element aus $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ ein Kubus ist.

Ist $x^3 = 3$ in $\mathbb{Z}/p\mathbb{Z}$ lösbar, so ist nach Theorem 2.1.17 $x^3 = 3$ auch in $\mathbb{Q}_p$ lösbar. Sei $\alpha \in \mathbb{Q}_p$ mit $\alpha^3 = 3$ In diesem Fall ist $(\frac{1}{\alpha}, 1, -1)$ Lösung der Selmer Gleichung.

Falls $x^3 = 3$ keine Lösung in $\mathbb{Z}/p\mathbb{Z}$ besitzt, so ist $p \equiv 1 \pmod 3$. Vertreter der Nebenklassen der Kuben in $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ sind $1, 3, 9$. Daher ist $a \not\equiv 0 \pmod p \implies a \equiv b^3 \pmod p \vee a \equiv 3b^3 \pmod p \vee a \equiv 9b^3 \pmod p$. Für $a = 5$:

- Falls $5 \equiv b^3 \pmod p$, so hat $x^3 - 5 = 0$ eine Lösung α in $\mathbb{Z}_p$ und $(-\alpha, \alpha, -1)$ ist eine Lösung von Selmer's Gleichung.
- Falls $5 \equiv 3b^3 \pmod p$, so hat $3x^3 - 5 = 0$ eine Lösung $\beta \in \mathbb{Z}_p$ und $(\beta, 0, -1)$ löst die Selmer Gleichung.
- Falls $5 \equiv 9b^3 \pmod p \overset{p\neq 3}{\iff} x^3 \equiv 15 \pmod p$ lösbar ist, so existiert ein γ aus $\mathbb{Z}_p$ mit $\gamma^3 \equiv 15 \pmod p$ und $(3\gamma, 5, -7)$ löst die Selmer Gleichung.

- Es verbleibt zu zeigen, dass $3x^3 + 4y^3 + 5z^3 = 0$ hat keine Lösung $\neq (0,0,0)$ über $\mathbb{Q}$. Dafür genügt es zu zeigen, dass

$$x^3 + 6y^3 = 10z^3 \tag{2.5}$$

keine rationale Lösung $\neq (0,0,0)$ hat.

Die Idee für den Beweis ist: Untersuche Gleichung (2.5) in $\mathbb{Q}(\sqrt[3]{6})$ und faktorisiere die Gleichung als $(x + \alpha y)(x^2 - \alpha xy + \alpha^2 y^2)$, wobei $\alpha = \sqrt[3]{6}$.

Für diesen Beweis braucht man allerdings einige algebraische Zahlentheorie, der wird in dieser Vorlesung ausgelassen.

2.3.1 Anwendung von Theorem 2.3.9 auf □ + □ + □

Behauptung: $Q(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$ stellt alle $n \in \mathbb{N}$ dar, außer diejenigen der Gestalt $4^i(7 + 8k)$ (siehe Theorem 1.5.7).

- Q stellt alle $x > 0$ über $\mathbb{R}$ dar.
- für $p \neq 2$ ist $Q(x_1, x_2, x_3)$ isotrop über $\mathbb{Q}_p$.

Lemma 2.3.12:
Q stellt $b \in \mathbb{Q}_2^*$ dar, falls $b\mathbb{Q}_2^{*2} \neq 7\mathbb{Q}_2^{*2}$ in $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$.

Beweis. Da die Darstellbarkeit von b nur von der Quadratrestklasse abhängt, ist oBdA $b = u \cdot 2^n$ mit $\{0,1\}, u \in \{1,3,5,7\}$. Wir verifizieren zunächst

$$\begin{aligned} 1 &= 1^2 + 0^2 + 0^2 \\ 3 &= 1^2 + 1^2 + 1^2 \\ 5 &= 2^2 + 1^2 + 0^2 \\ 2 &= 1^2 + 1^2 + 0^2 \\ 6 &= 2^2 + 1^2 + 1^2 \\ 10 &= 3^2 + 1^2 + 0^2 \\ 14 &= 3^2 + 2^2 + 1^2. \end{aligned}$$

Behauptung: 7 ist nicht darstellbar. Angenommen $x_1^2 + x_2^2 + x_3^2 = 7$ mit $x_1, x_2, x_3 \in \mathbb{Q}_2$. Durch Multiplikation mit dem Hauptnenner der x_i ist diese Gleichung zurückzuführen auf

$$x_1^2 + x_2^2 + x_3^2 = 4^i \cdot 7 \text{ mit } x_1, x_2, x_3 \in \mathbb{Z}_2.$$

OBdA ist $x_1 \equiv 1 \pmod 2$. Betrachte Gleichung $\mod 8$: $4^i 7 \equiv 0, 4, 7 \pmod 8$. Quadrate sind $\equiv 0, 1, 4 \pmod 8$ und $x_1^2 \equiv 1 \pmod 8$. Also $1 + x_2^2 + x_3^2 \equiv 0, 4, 7 \pmod 8$, was unlösbar ist. □

Proposition 2.3.13:
b ist genau dann von $Q = x_1^2 + x_2^2 + x_3^2$ darstellbar, wenn $b > 0$ und $b\mathbb{Q}_2^{*^2} \neq 7\mathbb{Q}_2^{*^2}$ in $\mathbb{Q}_2^* / \mathbb{Q}_2^{*^2}$.

Beweis. b wird über $\mathbb{Q}/\mathbb{R}/\mathbb{Q}_p$ genau dann von Q dargestellt, wenn $Q - by^2$ isotrop über $\mathbb{Q}/\mathbb{R}/\mathbb{Q}_p$ ist. (Denn wir können annehmen, dass für Lösungen x_1, x_2, x_3, y von $Q - bY^2 = 0 \quad y = 1$ gilt.)□

Satz 2.3.14 (Davenport / Cassels):
Sei $B(x,y) = \sum_{i,j}^r a_{ij} x_i y_j$ eine positiv definite, symmetrische Bilinearform mit $a_{ij} \in \mathbb{Z}$. Für die zugehörige quadratische Form $Q(x) := B(x,x)$ gelte:

$$\forall x \in \mathbb{Q}^r : \exists y \in \mathbb{Z}^r \text{ mit } Q(x-y) < 1.$$

Dann stellt Q jedes Element $b \in \mathbb{Z}$, das über $\mathbb{Q}$ dargestellt wird auch über $\mathbb{Z}$ dar.

Beweis. Sei $x = (x_1, \ldots, x_r) \in \mathbb{Q}^r \setminus \{0\}$ mit $Q(x) = b$. Sei

$$k := \mathrm{kgV}(\mathrm{Nenner}(x_1), \ldots, \mathrm{Nenner}(x_r)).$$

Falls $k = 1$: ✓ Falls $k > 1$, so zeigen wir: $\exists x' \in \mathbb{Q}^r \setminus \{0\}$ mit $Q(x') = b$ und

$$\mathrm{kgV}(\mathrm{Nenner}(x_1'), \ldots, \mathrm{Nenner}(x_r')) < k.$$

Nach Voraussetzung $\exists y \in \mathbb{Z}^r$ mit $Q(\underbrace{x-y}_{z}) < 1$. $z := x - y \in \mathbb{Q}^r \setminus \mathbb{Z}^r$. Da B positiv definit ist, gilt $0 < Q(z) = B(x-y, x-y) < 1$.

Wir definieren:

$$\begin{aligned} n &:= Q(y) - b \\ m &:= 2k(b - B(x,y)) = 2kb - 2B(kx, y) \\ k' &:= nk + m \\ x' &:= \frac{nkx + my}{k'} \end{aligned}$$

Dann gilt $n, m, k', nkx + my \in \mathbb{Z}$ bzw $\mathbb{Z}^r$.

Behauptung: $Q(x') = b$.

$$\begin{aligned} Q(x') = B(x', x') &= \frac{n^2k \overbrace{Q(x)}^{B(x,x)} + 2knmB(x,y) + m^2 \overbrace{Q(y)}^{B(y,y)}}{k'^2} \\ &= \frac{n^2k^2b + 2knm(b - \frac{m}{2k}) + m^2(n+b)}{k'^2} \\ &= \frac{n^2k^2b + 2kmnb + m^2b}{k'^2} \\ &= \frac{b(n^2k^2 + 2kmn + m^2)}{k'^2} = b \end{aligned}$$

$nkx + my \in \mathbb{Z}^r \implies \text{kgV}(\text{Nenner}(x_i'))$ teilt k'. Um den Beweis abzuschließen zeigen wir $0 < k' < k$.

$$\begin{aligned} \frac{k'}{k} &= nk + mk \\ &= n + \frac{m}{k} \\ &= Q(y) - b + 2(b - B(x,y)) \\ &= \overbrace{b}\ Q(x) - 2B(x,y) + Q(y) \\ &= Q(x - y) \in (0,1) \end{aligned}$$

□

Voraussetzungen für die Anwendung des Theorem 2.3.14 auf $Q = x_1^2 + x_2^2 + x_3^2$ sind erfüllt: $\forall (x_1, x_2, x_3) \in \mathbb{Q}^3 \colon \exists (y_1, y_2, y_3) \in \mathbb{Z}^3 \colon \sum_{i=1}^3 (x_i - y_i)^2 < 1$. Wähle y_i ganz mit $x_i - y_i \leq \frac{1}{2} \implies \sum_{i=1}^3 (x_i - y_1)^2 \leq \frac{3}{4} < 1$.

Drei Quadrate Satz $\implies$ Vier Quadrate Satz

$n \neq 4^i(8k+7) \implies n = \square + \square + \square + 0$

$n = 4^i(8k+7) \implies n - 1 = \square + \square + \square \implies n = \square + \square + \square + 1$

Aufgaben:

Zeige: jedes $n \in \mathbb{N}$ ist Summe von drei Dreieckszahlen, $0, 1, 3, 6, 10, \ldots$, das heißt Zahlen der Form $\frac{l(l+1)}{2}$, $l \in \mathbb{N}$. (Hinweis: Stelle $8n + 3$ als Summe von drei $\square$ dar.)

3 Der Dirichlet'sche Primzahlsatz

3.1 Charaktere abelscher Gruppen

Definition 3.1.1:

Sei G eine abelsche Gruppe, $\hat{G} := \mathrm{Hom}_{\mathbb{Z}}(G, T)$ heißt die Charaktergruppe von G. ($T = \{z \in \mathbb{C} : |z| = 1\}$) $\hat{G}$ ist abelsch, $\hat{G} = \{\chi : G \to T : \chi(x \circ y) = \chi(x)\chi(y) \forall x, y \in G\}$. $(\chi\chi')(x) = \chi(x)\chi'(x)$, $\chi(x) = 1$ ist das neutrale Element.

Dieses χ heißt Hauptcharakter. $\overline{\chi}(x) = \overline{\chi(x)}$ ist der zu χ inverse Charakter.

- $G \cong G' \implies \hat{G} \cong \hat{G}'$ denn $\mathrm{Hom}_{\mathbb{Z}}(G, T) \cong \mathrm{Hom}_{\mathbb{Z}}(G', T)$
- $G_1, G_2 \implies \widehat{G_1 \times G_2} \cong \hat{G}_1 \times \hat{G}_2$ da $\mathrm{Hom}_{\mathbb{Z}}(G_1 \times G_2, T) \cong \mathrm{Hom}_{\mathbb{Z}}(G_1, T) \times \mathrm{Hom}_{\mathbb{Z}}(G_2, T)$

Lemma 3.1.2:

$$\begin{aligned} \psi : T &\to \hat{\mathbb{Z}} \\ t &\mapsto \psi(t) : n \mapsto t^n \end{aligned}$$

ist ein Isomorphismus.

Beweis.

- $\psi(t) \in \hat{\mathbb{Z}}$: $\psi(t)(m+n) = t^{m+n} = t^m \cdot t^n = \psi(t)(m)\psi(t)(n)$
- ψ ist ein Homomorphismus: $\psi(tt')(n) = (tt')^n = t^n t'^n = \psi(t)(n) \cdot \psi(t')(n) = (\psi(t) \cdot \psi(t'))(n)$
- ψ ist injektiv: Sei $\psi(t)(n) = 1 \forall n \in \mathbb{Z} \implies \psi(t)(1) = 1 \implies t^1 = t = 1$.
- ψ ist surjektiv: Sei $\chi \in \hat{\mathbb{Z}}$ beliebig. Setze $t := \chi(1) \in T \implies \chi(n) = \chi(\underbrace{1 + \cdots + 1}_{n \text{ mal}}) = \chi(1)^n = t^n$ für $n \in \mathbb{N}$. $n < 0$: $\chi(n) = \chi(-n)^{-1} = (t^{-n})^{-1} = t^n \implies \psi(t)(n) = \chi(n) \forall n \in \mathbb{Z} \implies \psi(t) = \chi$. □

Definition 3.1.3:
Sei G eine abelsche Gruppe, $H \leq G$.

$$H^\perp := \{\chi \in \hat{G} \colon \chi(x) = 1 \forall x \in H\}$$

heißt die zu H orthogonale Gruppe.

$\psi \colon \hat{G} \to \hat{H}$ ist Homomorphismus mit Kern $H^\perp$. Also ist $H^\perp \leq \hat{G}$.
$\chi \mapsto \chi|_H$

Proposition 3.1.4:
Sei G abelsche Gruppe, $H \leq G$. Dann gilt:

$$\begin{aligned} \phi \colon H^\perp &\to \widehat{G/H} \\ \chi &\mapsto \phi(\chi) \colon x + H \mapsto \chi(x) \end{aligned}$$

ist ein Isomorphismus.

Beweis.
- $\phi(\chi)$ ist wohldefiniert: sei $x + H = x' + H \implies x - x' \in H \implies \chi(x - x') = 1 \implies \chi(x - x')\chi(x') \implies \chi(x) = \chi(x')$.
- $\phi(\chi)$ ist Homomorphismus (also $\in \widehat{G/H}$): $\phi(\chi)((x + H) + (y + H)) = \phi(\chi)(x + y + H) = \chi(x + y) = \chi(x)\chi(y) = \phi(\chi)(x + H)\phi(\chi)(y + H)$
- ϕ ist Homomorphismus: $\phi(\chi) \cdot \phi(\chi')(x + H) = \phi(\chi)(x + H) \cdot \phi(\chi')(x + H) = \chi(x)\chi'(x) = \chi\chi'(x) = \phi(\chi\chi')(x + H) \forall x \in G \implies \phi(\chi)\phi(\chi') = \phi(\chi\chi')$.
- ϕ ist injektiv: Sei $\phi(\chi) \equiv 1$, das heißt $\underbrace{\phi(\chi)(x + H)}_{\chi(x)} = \forall x \in G \implies \chi \equiv 1$.
- ϕ ist surjektiv: Sei $\psi \in \widehat{G/H}$. Setze $\chi \colon G \to T$, $x \mapsto \psi(x + H)$. Dann ist $\chi \in \hat{G}$, denn $\chi(x + y) = \psi(x + y + H) = \psi((x + H) + (y + H)) = \psi(x + H)\psi(y + H) = \chi(x)\chi(y)$. $\chi \in H^\perp$, denn $x \in H \implies \psi(x + H) = \psi(\underbrace{H}_{0 \in G/H}) = 1$. $\phi(\chi)(x + H) = \chi(x) = \psi(x + H) \forall x \in G \implies \phi(\chi) = \psi$

□

Korollar 3.1.5:

$$|G| < \infty \implies G \cong \hat{G}.$$

Beweis. Sei zunächst G zyklisch. Sei $|G| = n$. OBdA sei $G = \mu_n = \{t \in T : t^n = 1\}$. $\psi : T \to \hat{\mathbb{Z}}$, $t \mapsto \psi(t) : n \mapsto t^n$ ist nach Theorem 3.1.2 ein Isomorphismus.

$$\begin{aligned}
\psi(G) &= \{x \in \hat{\mathbb{Z}} : \chi(n) = 1\} \\
&= \{\chi \in \hat{\mathbb{Z}} : \forall k \in \mathbb{Z} : \chi(n)^k = 1\} \\
&= \{\chi \in \hat{\mathbb{Z}} : \forall k \in \mathbb{Z} : \chi(nk) = 1\} \\
&= \{\chi \in \hat{\mathbb{Z}} : \chi(n\mathbb{Z}) = 1\} \\
&= H^\perp \text{ für } H = n\mathbb{Z} \leq \mathbb{Z}.
\end{aligned}$$

$\implies G \overset{3.1.2}{\cong} \psi(G) = H^\perp \overset{3.1.4}{\cong} \widehat{\mathbb{Z}/H} = \widehat{\mathbb{Z}/n\mathbb{Z}} \cong \hat{G}$

Für G beliebig gilt $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ nach dem Hauptsatz für endliche abelsche Gruppen[1]. $\implies \hat{G} \cong \widehat{\mathbb{Z}/n_1\mathbb{Z}} \times \cdots \times \widehat{\mathbb{Z}/n_k\mathbb{Z}} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} = G$ □

Proposition 3.1.6:

Sei G eine abelsche Gruppe, $H \leq G$. Dann gilt

$$\begin{aligned}
\psi : \hat{G} &\to \hat{H} \\
\chi &\mapsto \chi|_H
\end{aligned}$$

ist Epimorphismus mit Kern $H^\perp$.

Beweis wird ausgelassen.
Insbesondere gilt:

$$\hat{G}/H^\perp \cong \hat{H}.$$

Korollar 3.1.7:

G abelsche Gruppe, $x \in G, x \neq 0$. Dann existiert ein $\chi \in \hat{G} : \chi(x) \neq 1$ (das heißt $\hat{G}$ ist punktetrennend).

[1] Leonhard Summerer. *Algebra*. 2022. URL: https://anton.mosich.at/Algebra.pdf, Satz 1.5.12.

Beweis. Sei $\langle x \rangle =: H$ die von x erzeugte zyklische Untergruppe von G. Dann ist $|H| > 1$. Wegen $H \cong \hat{H}$ folgt $\left|\hat{H}\right| > 1$. Dann existiert ein $\chi \in \hat{H}$ mit $\chi(x) \neq 1$. Nach Theorem 3.1.6 existiert $\tilde{\chi} \in \hat{G}$ mit $\tilde{\chi}|_H = \chi$, also $\tilde{\chi}(x) \neq 1$. □

Satz 3.1.8 (Orthogonalitätsrelationen):

Sei G endliche abelsche Gruppe und χ_0 sei der Hauptcharakter in $\hat{G}$. Dann gilt

1. $\chi \in \hat{G}$: $\sum_{x \in G} \chi(x) = \begin{cases} |G| & \text{falls } \chi = \chi_0 \\ 0 & \text{falls } \chi \neq \chi_0 \end{cases}$
2. $x \in G$: $\sum_{\chi \in \hat{G}} = \begin{cases} |G| & \text{falls } x = 0 \\ 0 & \text{falls } x \neq 0 \end{cases}$

Beweis. 1. $\chi = \chi_0$ ✓

$\sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(x + x_0) = \sum_{x \in G} \chi(x)\chi(x_0) = \chi(x_0) \cdot \sum_{x \in G} \chi(x)$. Wählt man x_0 so, dass $\chi(x_0) \neq 1$ (nach Theorem 3.1.7 möglich) so folgt $\sum_{x \in G} \chi(x) = 0$

2. $x = 0$ ✓

Wähle χ' mit $\chi'(x) \neq 1$.

$$\sum_{\chi \in \hat{G}} \chi(x) = \sum_{\chi \in \hat{G}} \chi\chi'(x) = \sum_{\chi \in \hat{G}} \chi(x)\chi'(x) = \underbrace{\chi'(x)}_{\neq 0} \cdot \sum_{\chi \in \hat{G}} \chi(x).$$

Daraus folgt $\sum_{\chi \in \hat{G}} \chi(x) = 0$. □

3.2 Dirichlet Charaktere

Definition 3.2.1:

Sei $m \in \mathbb{N}$, $\chi \colon \mathbb{Z} \to \mathbb{C}$ ($\chi \not\equiv 0$ muss wegen Punkt 3 nicht gefordert werden) hat folgende Eigenschaften:

1. $\chi(k \cdot l) = \chi(k) \cdot \chi(l)$
2. $\chi(k + m) = \chi(k)$
3. $\chi(k) = 0 \iff \operatorname{ggT}(k, m) > 1$

Dann heißt χ Dirichlet Charakter mod m. Die Menge aller Dirichlet Charaktere mod m wird mit Γ_m bezeichnet.

Punkt 2 $\implies$ χ ist festgelegt durch die Werte auf $0, 1, \ldots, m-1$. Punkt 3 $\implies$ es genügt prime Restklassen $\bmod m$ zu betrachten. Aus Punkt 1 folgt $\chi(1) = 1$. Aus $k^{\varphi(m)} \equiv 1 \pmod{m}$ für $(k,m) = 1$ folgt $\chi(k^{\varphi(m)}) \overset{1}{=} \chi(k)^{\varphi(m)} = \chi(1) = 1$ und somit $\chi\colon \mathbb{Z} \to T$.

Für $\chi \in \Gamma_m$ betrachten wir $\varphi\colon \left(\mathbb{Z}/m\mathbb{Z}\right)^* \to T$ $\quad k + m\mathbb{Z} \mapsto \chi(k)$. Dadurch ist φ eindeutig bestimmt. $\varphi \in \left(\widehat{\mathbb{Z}/m\mathbb{Z}}\right)^*$ wegen Punkt 1 für χ.

Proposition 3.2.2:

Sei $m \in \mathbb{N}$, dann ist Γ_m eine abelsche Gruppe bezüglich $\chi\chi'(k) := \chi(k)\chi'(k)$.

$$\begin{aligned}\psi\colon \Gamma_m &\to \left(\mathbb{Z}/m\mathbb{Z}\right)^* \\ x &\mapsto \varphi\colon k + m\mathbb{Z} \mapsto \chi(k) \text{ für } (k,m) = 1\end{aligned}$$

ist ein Isomorphismus

Beweis.

- Γ_m ist Gruppe: Seien $\chi, \chi' \in \Gamma_m$.
  - $\chi\chi'$ erfüllt Punkt 1, da das Produkt multiplikativer wieder multiplikativ ist.
  - $\chi\chi'(k+m) = \chi(k+m)\chi'(k+m) = \chi(k)\chi'(k) = \chi\chi'(k)$ (Punkt 2 ✓)
  - $\chi\chi'(k) = 0 \iff \chi(k) = 0 \vee \chi'(k) = 0 \iff (k,m) \neq 1$ (Punkt 3 ✓)
  - $\chi\bar{\chi}$ ist Einselement in Γ_m, $\chi\bar{\chi} =: \chi_0$ mit $\chi_0(k) = 1 \forall k$ mit $(k,m) = 1$.
  - $\bar{\chi}$ ist zu χ invers.
- ψ ist Isomorphismus:
  - ψ ist Homomorphismus: $\psi(\chi\chi')(k + m\mathbb{Z}) = \chi\chi'(k) = \chi(k)\chi'(k) = \psi(\chi)(k + m\mathbb{Z})\psi(\chi')(k + m\mathbb{Z}) \implies \psi(\chi\chi') = \psi(\chi)\psi(\chi')$.
  - ψ ist injektiv: $\psi(\chi)(k + m\mathbb{Z}) = 1 \forall k \iff \chi(k) = 1 \forall k \iff \chi = \chi_0$
  - ψ ist surjektiv: Sei $\varphi \in \left(\mathbb{Z}/m\mathbb{Z}\right)^*$. Setze $\chi\colon \mathbb{Z} \to T$ $\quad k \mapsto \begin{cases} 0 & \text{ggT}(k,m) > 1 \\ \varphi(k + m\mathbb{Z}) & \text{sonst} \end{cases}$. Dieses $\chi \in \Gamma_m$: Punkt 3 ist nach Definition erfüllt.

$$\begin{aligned}\chi(kl) = 0 &\iff \text{ggT}(kl, m) > 1 \\ &\iff \text{ggT}(k,m) > 1 \vee \text{ggT}(l,m) \\ &\iff \chi(k) = 0 \vee \chi(l) = 0 \\ &\iff \chi(k)\chi(l) = 0\end{aligned}$$

Für $\mathrm{ggT}(kl, m) = 1$:

$$\begin{aligned}\chi(kl) &= \varphi(kl + m\mathbb{Z}) \\ &= \varphi((k + m\mathbb{Z})(l + m\mathbb{Z})) \\ &= \varphi(k + m\mathbb{Z})\varphi(l + m\mathbb{Z}) \\ &= \chi(k)\chi(l) \implies \textit{Punkt 1}\end{aligned}$$

$$\chi(k + m) = \begin{cases} 0 & \mathrm{ggT}(k + m, m) > 1 \\ \varphi(k + m + m\mathbb{Z}) & \text{sonst} \end{cases} = \chi(k) \implies \textit{Punkt 2}$$

Nach Konstruktion also $\psi(\chi) = \varphi \implies$ Surjektivität erledigt. □

Korollar 3.2.3:
Für $m \in \mathbb{N}$ gilt $|\Gamma_m| = \phi(m)$, wobei ϕ die eulersche ϕ-Funktion bezeichnet.

Beweis.

$$|\Gamma_m| = \left|\left(\widehat{\mathbb{Z}/m\mathbb{Z}}\right)^*\right| = \left|\left(\mathbb{Z}/m\mathbb{Z}\right)^*\right| = \phi(m).$$

□

Korollar 3.2.4 (Orthogonalitätsrelationen für Dirichlet Charaktere):

1. Sei $(k, m) = 1$. Dann gilt $\sum_{\chi \in \Gamma_m} \chi(k) = \begin{cases} \phi(m) & \text{falls } k \equiv 1 \pmod m \\ 0 & \text{sonst.} \end{cases}$
2. Sei $\chi \in \Gamma_m$. Dann gilt $\sum_{k=0}^{m} -1\chi(k) = \begin{cases} \phi(m) & \text{falls } \chi = \chi_0 \\ 0 & \text{sonst.} \end{cases}$

Beweis. 1.

$$\sum_{\chi \in \Gamma_m} \chi(k) = \sum_{\chi \in \Gamma_m} \psi(\chi)(k + m\mathbb{Z}) = \sum_{\zeta \in \left(\widehat{\mathbb{Z}/m\mathbb{Z}}\right)^*} \zeta(k + m\mathbb{Z})$$

$$\underset{\text{OR für } \hat{G}}{=} \left|\left(\widehat{\mathbb{Z}/m\mathbb{Z}}\right)^*\right| \cdot \delta_{1+m\mathbb{Z},k+m\mathbb{Z}}$$

2.

$$\begin{aligned}\sum_{k=0}^{m-1}\chi(k) &= \sum_{\substack{k=0\\ \mathrm{ggT}(k,m)=1}}^{m-1}\chi(k) = \sum_{\substack{k=0\\ \mathrm{ggT}(k,m)=1}}^{m-1}\psi(\chi)(k+m\mathbb{Z})\\ &= \sum_{\bar{k}\in\left(\mathbb{Z}/m\mathbb{Z}\right)^*}\psi(\chi)(\bar{k})\\ &\underset{\text{OR für }\hat{G}}{=} \left|\left(\widehat{\mathbb{Z}/m\mathbb{Z}}\right)^*\right|\cdot\delta_{\chi,\chi_0}\end{aligned}$$

□

Beispiel 3.2.5:

- $m=1, m=2$: $\chi\in\Gamma_m \implies \chi=\chi_0$
- $m=3$: 2 ist Primwurzel mod 3 $\implies$ es genügt $\chi(2)$ zu kennen um χ zu bestimmen.

$$\begin{array}{ccc}\chi(2)^2=1 \implies \chi(2)=1 \vee \chi(2)=-1\\ \downarrow \qquad\quad \downarrow\\ \chi=\chi_0 \qquad \chi_1: \begin{array}{l}1\mapsto 1\\ 2\mapsto -1\end{array}\end{array}$$

- $m=4$: $\chi_1(k)=(-1)^{\frac{k-1}{2}}\in\Gamma_4$, denn $(-1)^{\frac{kk'-1}{2}}\equiv(-1)^{\frac{k-1}{2}}(-1)^{\frac{k'-1}{2}} \pmod 2$. Dies ist erfüllt, da $\frac{kk'-1}{2}\equiv\frac{k-1}{2}+\frac{k'-1}{2} \pmod 2 \iff kk'-1\equiv k+k'-2 \pmod 4 \iff (k-1)(k'-1)\equiv 0 \pmod 4$ ✓
- $m=5$: 2 ist Primwurzel mod 5, $\chi(2)^4=1 \implies \chi(2)\in\{1,i,-1,-i\}$

k	1	2	3	4
$\chi_0(k)$	1	1	1	1
$\chi_1(k)$	1	-1	-1	1
$\chi_2(k)$	1	i	i	-1
$\chi_3(k)$	1	$-i$	i	-1

- $m=8$: $\chi_1(k)=(-1)^{\frac{k-1}{2}}$, $\chi_2(k)=(-1)^{\frac{k^2-1}{8}}$

$$\begin{aligned}(-1)^{\frac{(kk')-1}{8}} &\equiv (-1)^{\frac{k^2-1}{8}}(-1)^{\frac{k'^2-1}{8}} \pmod 2\\ (kk')^2-1 &\equiv k^2-1+k'^2-1 \pmod{16}\\ \iff kk'-k^2-k'^2+1 &\equiv 0 \pmod{16}\\ (k^2-1)(k'^2-1) &\equiv 0 \pmod{16}\\ &\implies \chi_2 \text{ Charakter}\end{aligned}$$

$\chi_3=\chi_1(k)\chi_2(k)$

Definition 3.2.6:

Sei $m \in \mathbb{N}, d \mid n, \chi \in \Gamma_m$. χ heißt $\mod d$ erklärt, falls $\exists \chi' \in \Gamma_d \colon \chi(k) = \chi'(k)$ für $\operatorname{ggT}(k, m) = 1$.

Proposition 3.2.7:

Sei $\chi \in \Gamma_m, d \mid m$. Dann sind folgende Aussagen äquivalent:

1. χ ist $\mod d$ erklärt.
2. Für $\operatorname{ggT}(k, m) = 1$ und $k \equiv 1 \pmod d \implies \chi(k) = 1$.

Beweis. Punkt 1 $\implies$ Punkt 2 ist klar. ✓

Punkt 2 $\implies$ Punkt 1: Sei $\omega \colon \left(\mathbb{Z}/m\mathbb{Z}\right)^* \to \left(\mathbb{Z}/d\mathbb{Z}\right)^*$ ist Epimorphismus. Sei $\varphi \in \widehat{\left(\mathbb{Z}/m\mathbb{Z}\right)^*}$, das

$$k + m\mathbb{Z} \mapsto k + d\mathbb{Z}$$

heißt $\varphi \colon \left(\widehat{\mathbb{Z}/m\mathbb{Z}}\right) \to T$

$$k + m\mathbb{Z} \mapsto \chi(k)$$

$$\begin{array}{ccc} \left(\mathbb{Z}/m\mathbb{Z}\right)^* & \xrightarrow{\omega} & \left(\mathbb{Z}/d\mathbb{Z}\right)^* \\ \downarrow{\scriptstyle \varphi} & \swarrow_{\varphi'} & \\ T & & \end{array}$$

Gesucht: φ', sodass das Diagramm kommutiert, das heißt $\varphi' \circ \omega = \varphi$. Nach der universellen Eigenschaft von Homomorphismen, muss $\ker \omega \subseteq \ker \varphi$ damit solch ein φ' existiert. $k + d\mathbb{Z} = 1 + d\mathbb{Z} \implies \chi(k) = 1$ nach Punkt 2 und daher ist $\varphi(k + m\mathbb{Z}) = 1 \iff k + m\mathbb{Z} \in \ker \varphi$. φ' entspricht $\chi' \in \Gamma_d$ mit $\chi(k) = \chi'(k) \forall k \in \left(\mathbb{Z}/m\mathbb{Z}\right)^*$ □

Satz 3.2.8:

Seien $m, n \in \mathbb{Z}$ mit $(m, n) = 1$. Dann ist $\omega \colon \Gamma_m \times \Gamma_n \to \Gamma_{mn}$ ein Gruppenhomomorphismus.

$$(\chi, \chi') \mapsto \chi\chi'$$

Beweis.

$$\Gamma_{mn} \cong \left(\mathbb{Z}/mn\mathbb{Z}\right)^* \cong \widehat{\left(\mathbb{Z}/m\mathbb{Z}\right)^* \times \left(\mathbb{Z}/n\mathbb{Z}\right)^*} \cong \widehat{\left(\mathbb{Z}/m\mathbb{Z}\right)^*} \times \widehat{\left(\mathbb{Z}/n\mathbb{Z}\right)^*} \cong \Gamma_m \times \Gamma_n$$ □

Beispiel 3.2.9:

Γ_{15}

	1	2	4	7	8	11	13	14	
χ_0	1	1	1	1	1	1	1	1	$\left.\begin{matrix}\\\\\\\\\end{matrix}\right\}$ $\chi \mod 5$
χ_1	1	i	-1	i	$-i$	1	$-i$	-1	
χ_2	1	-1	1	-1	-1	1	-1	1	
χ_3	1	$-i$	-1	$-i$	i	1	i	-1	
χ_4	1	-1	1	1	-1	-1	1	-1	$\left.\begin{matrix}\\\\\\\\\end{matrix}\right\}$ $\chi \mod 5 \cdot \chi_1 \mod 3$
χ_5	1	$-i$	-1	i	i	-1	$-i$	1	
χ_6	1	1	1	-1	1	-1	-1	-1	
χ_7	1	i	-1	$-i$	$-i$	-1	i	1	

Definition 3.2.10:

$m \in \mathbb{N}$, $\chi \in \Gamma_m$. $d \mid m$ sei minimal mit χ ist $\mod d$ erklärt. Dann heißt d der Führer von $\chi \mod m$ (f_χ).

Definition 3.2.11:

$\chi \in \Gamma_m$ heißt primitiv, falls $f_\chi = m$.

$\chi \in \Gamma_m$ heißt reell, falls $\chi(k) \in \{0, 1, -1\} \forall k$ ($\iff \chi^2 = \chi_0$). Es folgt: die reellen Charaktere bilden eine Untergruppe von Γ_m (der Kern von $\chi \mapsto \chi^2$).

Proposition 3.2.12:

Sei $\mathrm{ggT}(m, n) = 1$, $\chi \in \Gamma_m$, $\chi' \in \Gamma_n$. $f_{\chi\chi'}$ sei der Führer von $\chi\chi' \mod mn$. Dann gilt: $f_{\chi\chi'} = f_\chi \cdot f_{\chi'}$. Insbesondere ist $\chi\chi'$ primitiv $\iff \chi \& \chi'$ sind primitiv.

Für reelle Charaktere gilt: χ, χ' reell $\implies \chi\chi'$ reell. Sei $\chi\chi'$ reeller Charakter $\mod mn$. Dann ist $(\chi\chi')^2 = \chi_0 \mod mn$. Mit $\omega\colon (\chi, \chi') \mapsto \chi\chi'$ (Isomorphismus nach letzter Vorlesung) ist

$$(\chi\chi')^2 = \omega(\chi, \chi')^2 = \omega(\chi^2, \chi'^2) \implies \chi^2 = \chi_0 \mod m, \chi'^2 = \chi_0 \mod n.$$

Beispiel 3.2.13:

Γ_8.

$$\begin{aligned}\chi_0&\\ \chi_1(k) &= (-1)^{\frac{k-1}{2}}\\ \chi_2(k) &= (-1)^{\frac{k^2-1}{8}}\\ \chi_3(k) &= (-1)^{\frac{k-1}{2}}(-1)^{\frac{k^2-1}{8}}\end{aligned}$$

alle sind reell, χ_2 und χ_3 sind primitiv. χ_1 ist $\mod 4$ erklärt.

Proposition 3.2.14:

1. Sei $p \in \mathbb{P} \setminus \{2\}$, $\chi \in \Gamma_{p^k}$ primitiv & reell $\implies$ $k = 1$: $\chi(n) = (\frac{n}{p})$.
2. $p = 2$ $\chi \in \Gamma_{2^k}$ primitiv & reell. $\implies$ $k = 2, 3$

Satz 3.2.15:

Sei $m = 2^k m'$ mit m' ungerade. $\chi \in \Gamma_m$ ist primitiv und reell impliziert m' quadratfrei, $k \in \{2, 3\}$. Für n mit $(n, m) = 1$ gilt:

$$\begin{aligned}k = 0&\colon \chi(n) = (\frac{n}{m})\\ k = 2&\colon \chi(n) = (-1)^{\frac{n-1}{2}}\left(\frac{n}{m'}\right)\\ k = 3&\colon \chi(n) = \left(\frac{2}{n}\right)\left(\frac{n}{m'}\right) \text{ oder } (-1)^{\frac{n-1}{2}}\left(\frac{2}{n}\right)\left(\frac{n}{m'}\right).\end{aligned}$$

3.3 Zahlentheoretische Funktionen

Beispiel 3.3.1 (Zahlentheoretische Funktionen):

- $\phi(n) = \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^*\right|$
- $\tau(n) = \sum_{d|n} 1$
- $\sigma^k(n) = \sum_{d|n} d^k$

- Möbiusfunktion:

$$\mu(n) = \begin{cases} 1 & \text{für } n = 1 \\ 0 & \text{für } n \text{ nicht quadratfrei} \\ (-1)^k & \text{für } n = p_1 \cdots p_k \text{ mit } p_1, \ldots, p_k \text{ paarweise verschieden.} \end{cases}$$

- $\pi(n) = \sum_{p \leq n} 1$
- von Mangoldt Funktion:

$$\Lambda(n) = \begin{cases} \log p & \text{falls } n = p^\alpha \text{ mit } \alpha \geq 1 \\ 0 & \text{sonst.} \end{cases}$$

- $u(n) = 1$
- $I(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{sonst} \end{cases}$

Verknüpfungen:

$$+ \colon (f+g)(n) \coloneqq f(n) + g(n)$$
$$\star \colon (f \star g)(n) \coloneqq \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \qquad \text{Faltung}$$

Die zahlentheoretischen Funktionen zusammen mit $+, \star$ bilden einen kommutativen Ring mit Eins. (I ist das Einselement)

$(f \star g) \star h \stackrel{?}{=} f \star (g \star h)$.

$$\begin{aligned} ((f \star g) \star h)(n) &= \sum_{d|n} (f \star g)(d) h(\tfrac{n}{d}) \\ &= \sum_{d|n} \left(\sum_{d'|d} f(d') g\left(\frac{d}{d'}\right) \right) h\left(\frac{n}{d}\right) \\ &= \sum_{a,b,c \colon abc=n} f(a) g(b) h(c) = \cdots = (f \star (g \star h))(n) \end{aligned}$$

Beispiel 3.3.2:

- $(u \star u)(n) = \sum_{d|n} 1 = \tau(n)$
- $(\Lambda \star u)(n) = \sum_{d|n} \Lambda(d)$ Für $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$:

$$\sum_{d|n} \Lambda(n) = \alpha_1 \log p_1 + \cdots + \alpha_k \log p_k = \log n$$

- Für $n \neq 1$:

$$\begin{aligned}(\mu \star u)(n) &= \sum_{d|n} \mu(d) \\ &= \binom{k}{0}(1) + \binom{k}{1}(-1) + \binom{k}{2}(1) + \binom{k}{3}(-1) + \cdots + \binom{k}{k}(-1)^k \\ &= (1-1)^k = 0\end{aligned}$$

Für $n = 1$: $(\mu \star u)(n) = 1 \implies \mu \star \nu = I$

Aufgaben:

Zeige, dass $(\phi \star u)(n) = n$.

Welche zahlentheoretischen Funktionen sind Einheiten?

Satz 3.3.3:

Ist f eine zahlentheoretische Funktion mit $f(1) \neq 0$, so ist f invertierbar.

Beweis.

$$f^{-1}(1) := \frac{1}{f(1)}$$

$$\text{induktiv: } f^{-1}(n) := \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d)$$

Dann gilt $f \star f^{-1} = I$, denn für $n = 1$: $(f \star f^{-1})(1) = f(1)f^{-1}(1) = 1$ und für $n \neq 1$ gilt:

$$\begin{aligned}(f \star f^{-1})(n) &= \sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) \\ &= f(1)f^{-1}(n) + \underbrace{\sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d)}_{-f(1)f^{-1}(n) \text{ nach Definition}} = 0\end{aligned}$$

□

Korollar 3.3.4:

Die zahlentheoretischen Funktionen mit $f(1) \neq 0$ bilden eine Gruppe bezüglich $\star$. Es gilt $(f \star g)^{-1} = f^{-1} \star g^{-1}$.

Definition 3.3.5:

Eine zahlentheoretische Funktion f heißt multiplikativ, falls $f \not\equiv 0$ und $\forall m, n$ mit $\mathrm{ggT}(m, n) = 1$ gilt $f(m)f(n) = f(mn)$. (Ohne Voraussetzung $\mathrm{ggT}(m, n) = 1$ sogar stark multiplikativ).

Eine multiplikative zahlentheoretische Funktion ist durch ihre Werte an allen Primzahlpotenzen eindeutig bestimmt.

Aufgaben:

f, g seien multiplikativ $\implies$ $f \star g$ ist multiplikativ.

Für multiplikative Funktionen gilt $f(1) = 1$ (denn $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$). Diese bilden eine Untergruppe der invertierbaren zahlentheoretischen Funktionen.

3.4 Dirichletreihen

Definition 3.4.1:

Sei a eine zahlentheoretische Funktion. Dann heißt

$$L_a(s) := \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

für $s \in \mathbb{C}$ die a zugeordnete Dirichletreihe.

Es gilt:

- $L_a(s) + L_b(s) = L_{a+b}(s)$

•

$$\begin{aligned} L_a(s) \cdot L_b(s) &= \left(\sum_{n=1}^{\infty} \frac{a(n)}{n^s}\right)\left(\sum_{m=1}^{\infty} \frac{b(m)}{m^s}\right) \\ &= \sum_{M=1}^{\infty} \left(\sum_{mn=M} a(n)b(m)\right) \frac{1}{n^s}\frac{1}{m^s} \\ &= \sum_{M=1}^{\infty} \underbrace{\left(\sum_{n|M} a(n) b\left(\frac{M}{n}\right)\right)}_{(a\star b)(M)} \frac{1}{M^s} = L_{a\star b}(s) \end{aligned}$$

$s = \sigma + it$. $|n^s| = \left|e^{s\log n}\right| = \left|e^{(\sigma+it)\log n}\right| = \left|e^{\sigma \log n}\right| \left|e^{it\log n}\right| = n^\sigma$

Satz 3.4.2:

Sei a eine zahlentheoretische Funktion.

1. Wenn $\sum_{n=1}^{\infty} \frac{a(n)}{n_0^s}$ für ein $s_0 \in \mathbb{C}$ konvergiert, dann konvergiert $\sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ für alle $s \in \mathbb{C}$ mit $\Re(s) > \Re(s_0)$ und die Konvergenz ist kompakt und gleichmäßig.
2. Unter obiger Annahme ist $s \mapsto \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ eine holomorphe Funktion für $\Re(s) > \Re(s_0)$ und
$$\left(\sum_{n=1}^{\infty} \frac{a(n)}{n^s}\right) = \sum_{n=1}^{\infty} \frac{a(n)\log n}{n^s}$$
und diese Reihe konvergiert dort kompakt und gleichmäßig.
3. Sind a und b zahlentheoretische Funkionen, $L_a(s)$ und $L_b(s)$ beide konvergent für $\Re(s) > \Re(s_0)$, dann gilt: $L_a(s) = L_b(s) \implies a(n) = b(n) \forall n$
4. Unter dieser Annahme gilt: $L_a(s)L_b(s) = L_{a\star b}(s)$ und letztere Reihe konvergiert ebenfalls auf $\Re(s) > \Re(s_0)$.

Satz 3.4.3 (Satz von Hurwitz):

Sei $(f_n)_{n\geq 1}$ eine Folge holomorpher Funktionen mit $f_n \to f$ kompakt. Sind alle f_n ohne Nullstelle, so ist entweder $f \equiv 0$ oder f hat auch keine Nullstelle.

Definition 3.4.4:

Angenommen $\sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ konvergiere / divergiere nicht für alle $s \in \mathbb{C}$. Dann heißt $\sigma_a := \inf\{\Re(s) : \sum_{n=1}^{\infty} \frac{a(n)}{n^s} \text{ konvergiert}\}$ die Konvergenzabszisse von L_a und $\bar{\sigma}_a := \inf\{\Re(s) : \sum_{n=1}^{\infty} \frac{a(n)}{n^s} \text{ konvergiert absolut}\}$ die Abszisse der absoluten Konvergenz von L_a.

Bemerkung 3.4.5:

Es gilt $0 \leq \bar{\sigma}_a - \sigma_a \leq 1$. Angenommen

$$\sum_{n=1}^{\infty} \frac{a(n)}{n_0^s}$$

sei konvergent. Zu zeigen: $\sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ konvergiert absolut für $\Re(s) > s_0 + 1$.

$$\exists A > 0 : \left|\frac{a(n)}{n^{s_0}}\right| \leq A, \left|\frac{a(n)}{n^s}\right| = \underbrace{\left|\frac{a(n)}{n^{s_0}}\right|}_{\leq A} \cdot \left|\frac{1}{n^{s-s_0}}\right| \leq \frac{A}{n^{\sigma-\sigma_0}}.$$

Also $A \sum_{n=1}^{\infty} \frac{1}{n^{\sigma-\sigma_0}} < \infty$.

Satz 3.4.6:

Sei f eine multiplikative zahlentheoretische Funktion. Dann ist für jede Primzahl p die Reihe $\sum_{j=0}^{\infty} \frac{f(p^j)}{p^{js}}$ kompakt konvergent im Bereich $\Re(s) > \bar{\sigma}_f$. Es gilt:

$$\prod_p \left(\sum_{n=1}^{\infty} \frac{f(p^j)}{p^{js}}\right) \overset{\text{komp.}}{\to} \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

Beweis.

$$\left|\sum_{j=M}^{\infty} \frac{f(p^j)}{p^{js}}\right| \leq \sum_{j=M}^{\infty} \frac{|f(p^j)|}{p^{j\sigma}} \leq \sum_{j=M}^{\infty} \frac{|f(n)|}{n^{\sigma}} \to 0$$

gleichmäßig auf kompakter Teilmenge von $\Re(s) > \bar{\sigma}_f$.

Sei $p_1 < p_2 < \ldots$ die Folge der Primzahlen.

$$N_k := \{n \in \mathbb{N} : p \mid n, p \in \mathbb{P} \implies p \in \{p_1, \ldots, p_k\}\}.$$

$$\left|\prod_{\substack{p\le p_k\\ p\in\mathbb{P}}}\left(\sum_{j=1}^{\infty}\frac{f(p^j)}{p^{js}}\right)-\sum_{n=1}^{\infty}\frac{f(n)}{n^s}\right| = \left|\sum_{j_1=0}^{\infty}\cdots\sum_{j_k=0}^{\infty}\frac{f(p_1^{j_1})\cdots f(p_k^{j_k})}{p^{j_1 s}\cdots p^{j_k s}}-\frac{f(n)}{n^s}\right|$$

$$= \left|\sum_{j_1=0}^{\infty}\cdots\sum_{j_k=0}^{\infty}\frac{f(p_1^{j_1}\cdots p_k^{j_k})}{(p_1^{j_1}\cdots p_k^{j_k})^s}-\sum_{n=1}^{\infty}\frac{f(n)}{n^s}\right|$$

$$= \left|\sum_{n\in N_k}\frac{f(n)}{n^s}-\sum_{n=1}^{\infty}\frac{f(n)}{n^s}\right|$$

$$= \left|\sum_{n\notin N_k}\frac{f(n)}{n^s}\right| \le \sum_{n\ge p_k}\frac{|f(n)|}{n^\sigma} \overset{k\to\infty}{\to} 0 \text{ glm} \qquad \square$$

Korollar 3.4.7:

Gilt sogar f ist streng multiplikativ, so gilt:

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s} = \sum_{p}\left(1-\frac{f(p)}{p^s}\right)^{-1}.$$

Beweis. f streng multiplikativ $\implies \sum_{j=0}^{\infty}\frac{f(p^j)}{p^{js}} = \sum_{j=0}^{\infty}\left(\frac{f(p)}{p^s}\right)^j = \frac{1}{1-\frac{f(p)}{p^s}}$ und die Behauptung folgt aus vorigem Satz. $\square$

Definition 3.4.8:

$L_u(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} =: \zeta(s)$ heißt Zeta-Funktion für $\Re(s) > 1$.

Für $\Re(s) > 1$ gilt $\left|\sum_{n=1}^{\infty}\frac{1}{n^s}\right| \le \sum_{n=1}^{\infty}\frac{1}{n^\sigma}$ ist konvergent wegen dem Integralkriterium.

$$\zeta(s) = \prod_{p}\left(1-\frac{1}{p^s}\right)^{-1}.$$

Satz 3.4.9:

$\zeta(s) \neq 0$ für $\Re(s) > 1$. In diesem Bereich gilt:

$$\zeta(s) = s\int_1^{\infty}\lfloor x\rfloor x^{-s-1}dx,$$

woraus die Identität

$$\zeta(s) - \frac{1}{s-1} = 1 - s\int_1^\infty \frac{\{x\}}{x^{s+1}}dx$$

folgt, welche $\zeta(s)$ zu einer für $\Re(s) > 0$ mit Ausnahme des Pols bei $s = 1$ (mit Residuum 1) holomorphen Funktion analytisch fortsetzt.

Beweis. Es gilt $f_n := \prod_{p\le p_n}(1-\frac{1}{p^s})^{-1} \to \zeta(s)$ kompakt. Alle f_n sind ohne Nullstelle, $\zeta(s) \not\equiv 0 \overset{3.4.3}{\Longrightarrow}$ $\zeta(s)$ hat keine Nullstelle in $\Re(s) > 1$.

Sei für folgende Überlegung $\Re(s) > 2$ vorausgesetzt.

$$\begin{aligned}
\zeta(s) &= \sum_{n=1}^\infty \frac{n(n-1)}{n^s} \\
&= \sum_{n=1}^\infty \frac{n}{n^s} - \sum_{n=1}^\infty \frac{n-1}{n^s} \\
&= \sum_{n=1}^\infty \frac{n}{n^s} - \sum_{n=1}^\infty \frac{n}{(n+1)^s} \\
&= \sum_{n=1}^\infty n\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) \\
&= \sum_{n=1}^\infty ns\int_n^{n+1} x^{-s-1}dx \\
&= s\sum_{n=1}^\infty \int_n^{n+1} \lfloor x\rfloor x^{-s-1}dx \\
&= s\int_1 \infty \lfloor x\rfloor x^{-s-1}dx.
\end{aligned}$$

Im selben Bereich ist $s\int_1^\infty x x^{-s-1}dx = \frac{s}{s-1} = 1 + \frac{1}{s-1}$. Zusammen ergeben die beiden Identitäten:

$$\zeta(s) - \frac{1}{s-1} = s\int_1^\infty \lfloor x\rfloor x^{-s-1}dx + 1 - s\int_1^\infty x x^{-s-1}dx = 1 - s\int_1^\infty \frac{\{x\}}{x^{s+1}}dx.$$

Die rechte Seite ist für $\Re(s) > 0$ definiert und dort holomorph. □

Definition 3.4.10:

Für $\chi \in \Gamma_m$ heißt $L(s,\chi) = \sum_{n=1}^\infty \frac{\chi(n)}{n^s}$ für $\Re(s) > 1$ die χ zugeordnete L-Reihe.

$L(s,\chi)$ ist für $\Re(s) > 1$ wohldefiniert wegen $\left|\sum_{n=1}^\infty \frac{\chi(n)}{n^s}\right| \le \sum_{n=1}^\infty \frac{|\chi(n)|(=1)}{n^\sigma}$. Für $m = 1$ ist $L(\chi_0, s) = \zeta(s)$. Allgemein gilt $L(\chi,s) = \prod_p(1-\frac{\chi(p)}{p^s})^{-1}$

Satz 3.4.11:

Für $\Gamma_m \ni \chi = \chi_0$ kann $L(s, \chi_0)$ auf $\Re(s) > 0$ analytisch fortgesetzt werden mit der Ausnahme für $s = 1$, wo $L(s, \chi_0)$ einen einfachen Pol mit Residuum $\frac{\varphi(m)}{m}$ besitzt. Für $\Gamma_m \ni \chi \neq \chi_0$ ist die Fortsetzung auf ganz $\Re(s) > 0$ analytisch.

Beweis. $L(s, \chi_0) = \prod_p \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1} = \zeta(s) \cdot \prod_{p|m}(1 - \frac{1}{p^s})$ und diese Darstellung liefert die Fortsetzung von $L(s, \chi_0)$ auf $\Re(s) > 0$.

$$\operatorname{Res}_{s=1}(L(s, \chi_0)) = \lim_{s \to 1} \underbrace{(s-1)\zeta(s)}_{\to 1} \underbrace{\prod_{p|m} \left(1 - \frac{1}{p^s}\right)}_{\to \prod_{p|m}\left(1-\frac{1}{p}\right)} = \prod_{p|m} \left(1 - \frac{1}{p}\right) = \frac{\varphi(m)}{m}.$$

Für $\chi \neq \chi_0$ gilt: $\sum_{n=1}^{m} \chi(n) = 0 \implies \left|\sum_{n \leq x} \chi(n)\right| \leq m$. Daher gilt:

$$\left|\sum_{<\leq n \leq x} \frac{\chi(n)}{n^s}\right| \leq \frac{1}{y^\sigma} \cdot \left|\sum_{<\leq n \leq x} \chi(n)\right| \leq \frac{m}{y^\sigma} \overset{\text{für } \sigma > 0}{\to} 0,$$

sodass $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ konvergiert. □

3.5 Primzahlen in arithmetischen Progressionen

Eulers Beweis für $|\mathbb{P}| = \infty$ basiert auf der Idee: $\sum_{p \in \mathbb{P}} \frac{1}{p} = \infty \implies |\mathbb{P}| = \infty$.

Wenn s mit $\Re(s) > 1 \implies \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s)$. Sei $s > 1$ reell. Dann gilt:

$$\begin{aligned}
\log\left(\prod_p \left(1 - \frac{1}{p^s}\right)^{-1}\right) &= \sum_p \log\left(1 - \frac{1}{p^s}\right)^{-1} \\
&= \sum_p \sum_{n=1}^{\infty} \frac{p^{-ns}}{n} \\
&= \sum_p p^{-s} + \sum_p \sum_{n=2}^{\infty} \frac{p^{-ns}}{n}
\end{aligned}$$

Wir schauen uns den hinteren Term an:

$$\begin{aligned}
\sum_p \sum_{n=2}^{\infty} \frac{p^{-ns}}{n} < \sum_p \sum_{n=2}^{\infty} p^{-ns} = \sum_p p^{-2s}(1 - p^{-s})^{-1} = \sum_p \frac{1}{p^s(p^s - 1)} \\
< \sum_{n=2}^{\infty} \frac{1}{n^s(n^s - 1)} < \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1
\end{aligned}$$

Folglich gilt: $\left|\sum_p p^{-s} - \log(\zeta(s))\right| < 1$ und daher gilt: $\sum_p p^{-s} - \log\left(\frac{1}{s-1}\right)$ ist beschränkt für $s \to 1^+$.

Seien $k, l \in \mathbb{N}$ mit $(k, l) = 1$. Dann sei

$$\mathbb{P}_l := \{p \in \mathbb{P} : p \equiv l \pmod{k}\}$$

Wir wollen zeigen: $\sum_{p \in \mathbb{P}_l} \frac{1}{p} = \infty$. Dazu untersuchen wir die Funktion

$$P_l(s) := \sum_{p \in \mathbb{P}_l} \frac{1}{p^s} \text{ für } \Re(s) > 1$$

mit dem Ziel $s \to 1^+$.

Wir benötigen als Hilfsmittel:

Satz 3.5.1 (Abel'sche Summationsformel):

Für eine zahlentheoretische Funktion $a(n)$ und für $A(x) = \sum_{n \leq x} a(n)$ sowie eine Funktion $f : [y, x] \to \mathbb{R}$ stetig differenzierbar gilt:

$$\sum_{y < n \leq x} a(n) f(n) = A(x) f(x) - A(y) f(y) - \int_y^x A(t) f'(t) dt$$

Beweis. Es gilt

$$\begin{aligned}
\sum_{y<n\le x} a(n)f(n) &= \sum_{n=\lfloor y\rfloor+1}^{\lfloor x\rfloor} a(n)f(n)\\
&= \sum_{n=\lfloor y\rfloor+1} \lfloor x\rfloor(A(n)-A(n-1))f(n)\\
&= \sum_{n=\lfloor y\rfloor+1}^{\lfloor x\rfloor} A(n)f(n) - \sum_{n=\lfloor y\rfloor}^{\lfloor x\rfloor-1} A(n)f(n+1)\\
&= \sum_{\lfloor y\rfloor+1}^{\lfloor x\rfloor-1} A(n)(f(n)-f(n+1)) + A(\lfloor x\rfloor)f(\lfloor x\rfloor) - A(\lfloor y\rfloor)f(\lfloor y\rfloor+1)\\
&= -\sum_{\lfloor y\rfloor+1}^{\lfloor x\rfloor-1} A(n)\int_n^{n+1} f'(t)dt + A(\lfloor x\rfloor)f(\lfloor x\rfloor) - A(\lfloor y\rfloor)f(\lfloor y\rfloor+1)\\
&= -\sum_{\lfloor y\rfloor+1}^{\lfloor x\rfloor-1} \int_n^{n+1} A(t)f'(t)dt + A(\lfloor x\rfloor)f(\lfloor x\rfloor) - A(\lfloor y\rfloor)f(\lfloor y\rfloor+1)\\
&= -\int_{\lfloor y\rfloor+1}^{\lfloor x\rfloor} A(t)f'(t)dt + A(\lfloor x\rfloor)f(\lfloor x\rfloor) - A(\lfloor y\rfloor)f(\lfloor y\rfloor+1)\\
&= -\int_{\lfloor y\rfloor+1}^{\lfloor x\rfloor} A(t)f'(t)dt + A(x)f(x) - \int_{\lfloor x\rfloor}^{x} A(t)f'(t)dt - A(y)f(y)\\
&\qquad + \int_y^{\lfloor y\rfloor+1} A(t)f'(t)dt\\
&= -\int_y^x A(t)f'(t)dt + A(x)f(x) - A(y)f(y)
\end{aligned}$$

□

Proposition 3.5.2:
Sei $\Theta(x) := \sum_{p\le x}\log(p)$. Dann gilt: $\Theta(n) \le 2n\log(2)$ ($\implies$ insbesondere $\Theta(n) = \mathcal{O}(n)$).

Beweis. Betrachte den Ausdruck $\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!} =: M$. In $(1+1)^{2m+1} = \sum_{i=0}^{2m+1}\binom{2m+1}{i}$ kommt $\binom{2m+1}{m}$ zwei mal vor, das heißt $2M \le 2^{2m+1} \implies M \le 2^{2m}$.
Für $p \in \mathbb{P}$, $m+1 < p \le 2m+1$ gilt: $p \mid M$ und daher $\prod_{m+1<p\le 2m+1} p \mid M$.

$$\Theta(2m+1) - \Theta(m+1) = \sum_{m+1<p\le 2m+1} \log(p) \le \log(M) < 2m\log(2)$$

Wir zeigen nun $\Theta(n) \le 2n\log(2)$ durch Induktion nach n. Für $n = 1, 2$ ist das klar.

Angenommen $\Theta(n) < 2n\log(2)$ sei gezeigt für alle $n < n_0$. Falls $n_0 \equiv 0 \pmod 2$, dann ist $\Theta(n_0) = \Theta(n_0 - 1) < 2(n_0 - 1)\log(2) < 2n_0\log(2)$. Falls $n_0 \equiv 1 \pmod 2$, so ist $n_0 = 2m + 1$.

$$\Theta(n_0) = \underbrace{\Theta(2m-1) - \Theta(m-1)}_{<2m\log(2)} + \underbrace{\Theta(m+1)}_{<2m\log(2)}$$
$$\implies \Theta(n_0) < (4m+2)\log(2) = 2(2m+1)\log(2) = 2n_0\log(2) \qquad \square$$

Aufgaben:

Man leite mithilfe der Abel'schen Summationsformel her:

$$\sum_{p\le x} 1 =: \pi(x) = \mathcal{O}\left(\frac{x}{\log(x)}\right).$$

Hinweis: $a(n) = \log_n \delta_{n,\mathbb{P}}$ und $f(x) = \frac{1}{\log(x)}$.

Proposition 3.5.3:

$$\sum_{p^k\le x} \log(p) = \sum_{n\le x} \Lambda(n) = \mathcal{O}(x).$$

Beweis.

$$\sum_{p^k\le x} \log(p) = \underbrace{\sum_{p\le x} \log(p)}_{\Theta(x)} + \sum_{k\ge 2}\sum_{p\le \sqrt[k]{x}} \log(p).$$

Bemerke, dass $\Theta(y) < y\log(y)$ und $\sum_{p\le\sqrt[k]{x}} \log(p) = 0$, für $k > \frac{\log(x)}{\log(2)}$. Es liefern also höchstens $O(\log(x))$ Summanden einen Beitrag $\neq 0$.

$$\sum_{k\ge 2}\sum_{p\le\sqrt[k]{x}} \log(p) = \mathcal{O}\left(x^{\frac{1}{2}}\log(x)\log(x)\right) = \mathcal{O}\left(x^{\frac{1}{2}}\log^2(x)\right)^2.$$

Also gilt $\sum_{p^k\le x}\log(p) = \mathcal{O}(x)$. $\square$

Proposition 3.5.4:

$$\sum_{p\leq x}\frac{\log(p)}{p}=\log(x)+\mathcal{O}(1)$$

Beweis.

- $\sum_{d|n}\Lambda(d)=\Lambda\star u(n)=\log(n)$
- $\sum_{n\leq x}\log(n)=x\log(x)+\mathcal{O}(x)$ folgt aus Anwendung der Euler'schen Summenformel.

$$\sum_{n\leq x}\log(n)=\int_1^x\log(t)dt+\frac{\log(x)}{2}+\int_1^x(\lfloor t\rfloor-t)\frac{1}{t}dt.$$

Es gilt

$$\begin{aligned}\sum_{n\leq x}\log(n)&=\sum_{n\leq x}\sum_{d|n}\Lambda(d)\\&=\sum_{d\leq x}\frac{x}{d}\Lambda(d)+\mathcal{O}\left(\sum_{d\leq x}\Lambda(d)\right)\\&=x\sum_{d\leq x}\frac{\Lambda(d)}{d}+\mathcal{O}(x)\ (3.5.3)\end{aligned}$$

Es folgt (nach Teilen durch x): $\sum_{d\leq x}\frac{\Lambda(d)}{d}=\log(x)+\mathcal{O}(1)$.

$$\underbrace{\sum_{n\leq x}\frac{\Lambda(n)}{n}}_{\sum_{p^k\leq x}\frac{\log(p)}{p^k}}-\sum_{p\leq x}\frac{\log(p)}{p}$$

und die Differenz ist gerade

$$\sum_{\substack{p^k\leq x\\k\geq 2}}\frac{\log(p)}{p^k}\leq\sum_{\substack{p^k\leq x\\k\geq 2}}\frac{\log(p)}{p^2}\leq\sum_{n\leq x}\frac{\log(n)}{n^2}\leq\sum_{n\leq x}\frac{1}{n^{\frac{3}{2}}}=\mathcal{O}(1).$$

Daraus folgt $\sum_{p\leq x}\frac{\log(p)}{p}=\log(x)+\mathcal{O}(1)$ wie behauptet. □

k,l mit $\mathrm{ggT}(k,l)=1$, $\mathbb{P}_l=\{p\in\mathbb{P}|p\equiv l\pmod k\}$. $\sum_{p\in\mathbb{P}_l}\frac{1}{p}=\infty\rightarrow$ untersuche $\sum_{p\in\mathbb{P}_l}\frac{1}{p^s}$ für $\Re(s)=1$.

Satz 3.5.5:
Für $\chi \in \Gamma_k, \chi \neq \chi_0$ gilt $L(1,\chi) \neq 0$.

Beweis. Sei zunächst χ nicht reell. Setze $P(s) := \prod_{\chi \in \Gamma_k} L(s,\chi)$. Für $\delta < 1$ reell gilt:

$$\begin{aligned}
\log P(\delta) &= \sum_{\chi \in \Gamma_k} \log L(\delta,\chi) \\
&= \sum_{\chi \in \Gamma_k} \sum_{p} \log\left(1 - \frac{\chi(p)}{p^\delta}\right)^{-1} \\
&= \sum_{\chi \in \Gamma_k} \sum_{p} \sum_{m \geq 1} \frac{\chi(p^m)}{m p^{m\delta}} \\
&= \sum_{p} \sum_{m \geq 1} \frac{1}{m p^{m\delta}} \sum_{\chi \in \Gamma_k} \chi(p^m)
\end{aligned}$$

$$\text{Es ist } \sum_{\chi \in \Gamma_k} \chi(a) = \begin{cases} 0 & a \not\equiv 1 \pmod k \\ \varphi(k) & a \equiv 1 \pmod k \end{cases} \implies = \sum_{\substack{p_m \\ p \equiv 1 \pmod k}} \sum_{m \geq 1} \frac{\phi(k)}{m p^{m\delta}} \geq 0$$

$$\implies P(\delta) \geq 1$$

Angenommen es gelte $L(1,\chi) = 0$. Dann wäre auch $L(1,\overline{\chi}) = \overline{L(1,\chi)} = 0$. Weil χ nicht reell, folgt $\chi \neq \overline{\chi}$. Es folgte, dass $P(s)$ eine doppelte Nullstelle bei $s = 1$ hätte. $L(s,\chi_0)$ hat für $s = 1$ eine neinfachen Pol, sodass insgesamt $P(s)$ eine Nullstelle bei $s = 1$ hätte. Das ist ein Widerspruch zu $P(\delta) \geq 1$ für $\delta > 1$. □

Sei nun $\chi \neq \chi_0$ ein reeller Charakter. Definiere $f := \chi \star u$. Dann ist $f(n) = \sum_{d|n} \chi(d)$. Sei $f(s) := L_f(s)$. f ist multiplikativ. Es ist

$$f(p^m) = \sum_{l=0}^{m} \chi(p^l) = \begin{cases} 1 & \text{, falls } p \mid k \\ \geq 1 & \text{, falls } m \text{ gerade} \\ \geq 0 & \text{, falls } m \text{ ungerade.} \end{cases}$$

Es folgt $f(n) \geq 0 \forall n$ und $f(n) \geq 1$ falls n ein vollständiges Quadrat. Daher gilt $F(\delta) = \sum_{n=1}^{\infty} \frac{f(n)}{n^\delta} \geq \sum_{n=1}^{\infty} \frac{1}{n^{2\delta}} = \zeta(2\delta)$. Da ζ bei $s = 1$ einen Pol hat, ist $\delta_F \geq \frac{1}{2}$. Andererseits gilt: $F(s) = L_\chi(s) \cdot L_\chi(u) = L(s,\chi)\zeta(s)$. Wäre $L(1,\chi) = 0$, so folgte $F(s)$ wäre analytisch für $\Re(s) > 0$ und somit ergibt sich ein Widerspruch zu $\delta_F \geq \frac{1}{2}$.

Satz 3.5.6 (Dirichlet'scher Primzahlsatz):
Für $(k,l) = 1$ gilt $|\mathbb{P}_l| = \infty$.

Beweis.

1. Schritt: Es genügt zu zeigen, dass für $x \geq 3, \delta = 1 + \frac{1}{\log x}$ gilt

$$\sum_{p \equiv l \pmod k} \frac{1}{p^\delta} = \frac{1}{\phi(k)} \log\left(\frac{1}{\delta - 1}\right) + \mathcal{O}(1). \tag{3.1}$$

Sei $\Sigma_1 := \sum_{p \equiv l \pmod k} \frac{1}{p^\delta}, \Sigma_2 := \sum_{\substack{p \equiv l \pmod k \\ p \leq x}} \frac{1}{p}$. Dann ist $|\Sigma_1 - \Sigma_2| \leq \sum_{p \leq x} (\frac{1}{p} - \frac{1}{p^\delta}) + \sum_{p > x} \frac{1}{p^\delta}$.
Es ist

$$\begin{aligned}
\sum_{p \leq x} \left(\frac{1}{p} - \frac{1}{p^\delta}\right) &= \sum_{p \leq x} \frac{1 - p^{-\delta+1}}{p} \\
&= \sum_{p \leq x} \frac{1 - e^{-(\delta-1)\log p}}{p} \\
&\leq \sum_{p \leq x} \frac{(\delta - 1)\log p}{p} \\
&= \frac{1}{\log x} \underbrace{\sum_{p \leq x} \frac{\log p}{p}}_{\log x + \mathcal{O}(1)} = \mathcal{O}(1).
\end{aligned}$$

$$\begin{aligned}
\sum_{p > x} \frac{1}{p^\delta} \left(= \sum_{x=n}^{\infty} a(n) f(n) \text{ hier } f(x) = \frac{1}{x^\delta}, a(n) = \mathbb{1}_{\mathbb{P}}.\right) \\
&= \lim_{y \to \infty} \left(\sum_{x < n \leq y} \mathbb{1}_{\mathbb{P}}(n) \frac{1}{n^\delta} \right) \\
&= \lim_{y \to \infty} \left(\frac{1}{y^z} \sum_{p \leq y} 1 - \frac{1}{x^\delta} \sum_{p \leq x} 1 - \int_x^y \left(\sum_{p \leq t} 1 \right) \frac{-\delta}{t^{\delta+1}} dt \right) \\
&= \mathcal{O}(1) + \lim_{y \to \infty} \int_x^y \pi(t) \frac{\delta}{t^{\delta+1}} dt \\
&= \mathcal{O}(1) + \int_x^\infty \mathcal{O}\left(\frac{t}{\log t}\right) \frac{1}{t^{\delta+t}} dt \\
&= \mathcal{O}(1) + \mathcal{O}\left(\int_x^\infty \frac{1}{t^\delta \log t} dt \right) \\
t^\delta \log t \geq t^\delta \log x \implies &= \mathcal{O}(1) + \mathcal{O}\left(\frac{1}{\log x} \int_x^\infty \frac{dt}{t^\delta} \right) \\
&= \mathcal{O}(1) + \mathcal{O}\left(\frac{1}{\log x} \underbrace{\int_x^\infty \frac{dt}{t}}_{\log x} \right) = \mathcal{O}(1)
\end{aligned}$$

2. Schritt: Beweis von Gleichung (3.1). Für $\delta > 1$ gilt:

$$\sum_{p \equiv l \pmod k} \frac{1}{p^\delta} = \sum_p \frac{1}{p^\delta} \left(\frac{1}{\varphi(k)} \sum_{\chi \in \Gamma_k} \overline{\chi}(l) \chi(p) \right).$$

Es gilt nämlich

$$\sum_{\chi \in \Gamma_k} \overline{\chi}(l) \chi(p) = \sum_{\chi \in \Gamma_k} \chi(l^{-1}) \chi(p) = \sum_{\chi \in \Gamma_k} \chi(l^{-1}p) = \begin{cases} \varphi(k) & l^{-1}p \equiv 1 \pmod k \\ 0 & \text{sonst.} \end{cases}$$

$$\sum_{p \equiv l \pmod k} \frac{1}{p^\delta} = \frac{1}{\varphi(k)} \sum_{\chi \in \Gamma_k} \overline{\chi}(l) \sum_p \frac{\chi(p)}{p^\delta}.$$

$$\underbrace{\sum_p \sum_{m \geq 1} \frac{1}{m p^{m\delta}}}_{-\sum \log(1 - \frac{1}{p^\delta})} - \sum_p \frac{1}{p^\delta} = \sum_p \sum_{m \geq 2} \frac{1}{m p^{m\delta}} \leq \frac{1}{2} \sum_p \sum_{m \geq 2} \frac{1}{p^{m\delta}} = \frac{1}{2} \sum_p \frac{1}{p^\delta (p^\delta - 1)} = \mathcal{O}(1).$$

Folglich gilt für $\chi = \chi_0$

$$\begin{aligned} \sum_p \frac{\chi_0(p)}{p^\delta} &= \underbrace{\sum_p \sum_{m \geq 1} \frac{1}{m p^{m\delta}}}_{-\sum_p \log(1 - \frac{1}{p^\delta})} - \underbrace{\sum_{p \mid k} \sum_{m \geq 1} \frac{1}{m p^{m\delta}}}_{\mathcal{O}(1)} \\ &= \log \prod_p \left(1 - \frac{1}{p^\delta}\right)^{-1} + \mathcal{O}(1) \\ &= \log \zeta(\delta) + \mathcal{O}(1) \\ &= \log \left(\frac{1}{\delta - 1} \right) + \mathcal{O}(1) \end{aligned}$$

Für $\chi \neq \chi_0$:

$$\begin{aligned} \sum_p \frac{\chi(p)}{p^\delta} &= \sum_p \sum_{m \geq 1} \frac{\chi(p)^m}{m p^{m\delta}} + \mathcal{O}(1) \\ &= -\sum_p \log \left(\frac{1 - \chi(p)}{p^\delta} \right) + \mathcal{O}(1) \\ &= \log \prod_p \left(\frac{1 - \chi(p)}{p^\delta} \right)^{-1} + \mathcal{O}(1) \\ &= \log L(\delta, \chi) + \mathcal{O}(1) \end{aligned}$$

Da $\chi \neq \chi_0$ ist $L(\delta, \chi)$ analytisch für $\delta > 0$. Insbesondere ist $L(\delta, \chi)$ stetig bei 1. Also gilt $\lim_{\delta \to 1} L(\delta, \chi) = L(1, \chi) \neq 0$. Daher ist $\sum_p \frac{\chi(p)}{p^\delta} = \mathcal{O}(1)$. Es folgt: $\sum_{p \equiv l \pmod k} \frac{1}{p^\delta} = \frac{1}{\varphi(k)} \underbrace{\overline{\chi_0}(l)}_{=1} \log(\frac{1}{\delta - 1}) + \mathcal{O}(1)$. Mit $\delta \to 1^+$ folgt der Dirichlet'sche Primzahlsatz. □

Warnung:

Auch wenn ich mir in der Vorlesung gründlich Mühe gebe ordentlich mitzuschreiben, sind mit Sicherheit zahlreiche Tippfehler in meiner Mitschrift. Wenn dir einer auffällt, gib mir unbedingt Bescheid. Schreib dazu einfach per WhatsApp oder E-Mail (anton@mosich.at) wo der Fehler ist, und bestenfalls auch noch was richtig wäre.