Gitterpunktsatz von Minkowski

Tobias Hirsch

Würzburg 2022

Elemente der Vektorrechnung

Ein Vektor ist ein „Pfeil“ im $\mathbb{R}^2$. Schreibweise

$$\begin{pmatrix} 1 \\ \sqrt{2} \end{pmatrix},$$

Zwei Vektoren werden addiert, in dem man ihre einzelnen Koordinaten addiert

$$\begin{pmatrix} 1 \\ \sqrt{2} \end{pmatrix} + \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ \sqrt{2} \end{pmatrix}$$

Ebenfalls koordinatenweise erfolgt die Multiplikation eines Vektors mit einem Skalar (=reellen Zahl)

$$\sqrt{2} \cdot \begin{pmatrix} 1 \\ \sqrt{2} \end{pmatrix} = \begin{pmatrix} \sqrt{2} \\ 2 \end{pmatrix}$$

Der Mittelpunkt der Verbindungsstrecke zweier Punkte $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in \mathbb{R}^2$ ist gegeben durch

$$\frac{x+y}{2} = \frac{1}{2}\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) = \begin{pmatrix} \frac{x_1+y_1}{2} \\ \frac{x_2+y_2}{2} \end{pmatrix}$$

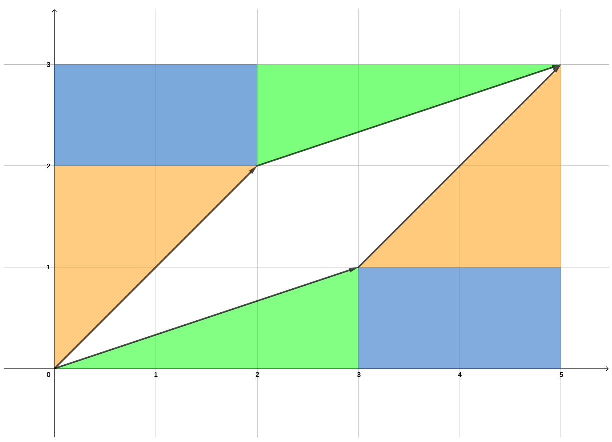
Zwei Vektoren $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ spannen im $\mathbb{R}^2$ ein Parallelogramm auf:

$$P\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) := \left\{a_1 \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + a_2 \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \mid a_1, a_2 \in [0,1]\right\}$$

Der Flächeninhalt dieses Parallelogramms ist gegeben durch

$$\mathrm{Vol}(P) = |x_1 y_2 - y_1 x_2|$$

Beweis für Vektoren im ersten Quadranten durch Bild:



$$(x_1+y_1)(x_2+y_2) - x_1x_2 - y_1y_2 - 2x_2y_1 = x_1y_2 - y_1x_2$$

Zwei Vektoren $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ heißen linear unabhängig, wenn für $a_1, a_2 \in \mathbb{R}$ aus

$$a_1 \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + a_2 \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 0$$

bereits $a_1 = a_2 = 0$ folgt, sonst sind sie linear abhängig.
Zwei Vektoren $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ sind genau dann linear abhängig, wenn

- einer der beiden der Nullvektor ist.
- sie parallel sind, also einer ein Vielfaches des anderen ist.

$$a_1 x + a_2 y = 0,\ a_1 \neq 0 \quad \Rightarrow \quad x = -\frac{a_2}{a_1} y$$
$$x = ay \quad \Rightarrow \quad x - ay = 0$$

- das von ihnen aufgespannte Parallelogramm Flächeninhalt 0 hat.

$$\mathrm{Vol}(P(x, y)) = 0$$

Lemma 1. *Sind* $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in \mathbb{R}^2$ *linear unabhängig, so existieren für jeden Vektor* $\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \in \mathbb{R}^2$ *eindeutig bestimmte* $a_1, a_2 \in \mathbb{R}$*, sodass*

$$a_1 \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + a_2 \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$

Beweis der Eindeutigkeit. Seien $a_1, a_2, b_1, b_2 \in \mathbb{R}$, sodass

$$a_1 \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + a_2 \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} v_1 \\ w_1 \end{pmatrix} = b_1 \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + b_2 \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

Dann gilt

$$(a_1 - b_1) \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + (a_2 - b_2) \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 0,$$

also wegen der linearen Unabhängigkeit $a_1 = b_1$ und $a_2 = b_2$. ▲

Gitter im $\mathbb{R}^2$

Definition 2 (Gitter)**.** Ein *Gitter* G im $\mathbb{R}^2$ ist eine Menge der Form

$$G = \{a_x \cdot x + a_y \cdot y \mid a_x, a_y \in \mathbb{Z}\}$$

wobei $x, y \in \mathbb{R}^2$ linear unabhängig sind. Die Vektoren $x, y \in \mathbb{R}^2$ heißen *Gitterbasis* von G.

Beispiel (nicht linear unabhängig)**.** Gitter entlang einer Geraden

Beispiel (Gitterbasis nicht eindeutig)**.** Für die Vektoren $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ erhält man genau die Punkte mit ganzzahligen Koordinaten - genauso für die Vektoren $\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ oder allgemeiner $\begin{pmatrix} a \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ mit $a \in \mathbb{Z}$. Die Gitterbasis zu einem gegebenen Gitter ist also nicht eindeutig.

Bemerkung. In obigen Beispiel ist in gewisser Weise $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ eine einfachere Gitterbasis als $\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Im Allgemeinen möchte man z.B. eine möglichst kurze Gitterbasis finden. Dies ist für allgemeine Gitter nicht einfach möglich. Zumindest eine Approximation daran erhält man mithilfe des LLL-Algorithmus.

Definition 3 (Grundmasche, Gittervolumen)**.** Für ein Gitter G mit Gitterbasis x, y heißt $P(x, y)$ *Grundmasche* des Gitters. Das Volumen der Grundmasche

$$\mathrm{Vol}(G) := \mathrm{Vol}(P(x, y))$$

heißt *Gittervolumen* von G.

Direkt nach Definition ist nicht klar, warum das Gittervolumen nur von Gitter und nicht auch von der konkreten Wahl der Gitterbasis abhängt. Das folgende Lemma weißt dies nach:

Lemma 4. *Für v, w und x, y Gitterbasen von G gilt* $\mathrm{Vol}(P(v,w)) = \mathrm{Vol}(P(x,y))$.

Beweis. Seien v, w und x, y zwei Gitterbasen von G. Dann existieren $a_x, a_y, b_x, b_y \in \mathbb{Z}$ mit $v = a_x \cdot x + a_y \cdot y, w = b_x \cdot x + b_y \cdot y$. Also gilt

$$\begin{aligned}\mathrm{Vol}(P(v,w)) &= |(a_x x_1 + a_y y_1)(b_x x_2 + b_y y_2) - (b_x x_1 + b_y y_1)(a_x x_2 + a_y y_2)| \\ &= |a_x x_1 b_x x_2 + a_x x_1 b_y y_2 + a_y y_1 b_x x_2 + a_y y_1 b_y y_2 - b_x x_1 a_x x_2 - b_x x_1 a_y y_2 - b_y y_1 a_x x_2 - b_y y_1 a_y y_2| \\ &= |a_x x_1 b_y y_2 + a_y y_1 b_x x_2 - b_x x_1 a_y y_2 - b_y y_1 a_x x_2| \\ &= |(a_x b_y - a_y b_x) x_1 y_2 - (a_x b_y - a_y b_x) y_1 x_2| = |a_x b_y - a_y b_x| \cdot |x_1 y_2 - y_1 x_2|\end{aligned}$$

Da in obiger Rechnung nur ganze Zahlen auftreten und $\mathrm{Vol}(P(v,w)) \neq 0$, folgt $|a_x b_y - a_y b_x| \geq 1$, also

$$\mathrm{Vol}(P(v,w)) \geq \mathrm{Vol}(P(x,y))$$

Analog erhält man auch $\mathrm{Vol}(P(v,w)) \leq \mathrm{Vol}(P(x,y))$, somit gilt die Behauptung. ▲

Der Gitterpunktsatz von Minkowski

Definition 5 (symmetrisch)**.** Eine Menge $M \subseteq \mathbb{R}^2$ heißt *punktsymmetrisch zum Ursprung*, wenn für alle $x \in M$ auch $-x \in M$.

Definition 6 (konvex)**.** Eine Menge $M \subseteq \mathbb{R}^2$ heißt *konvex*, wenn zwei Punkte $x, y \in M$ auch ihre Verbindungsstrecke in M liegt.

$$\{t \cdot x + (1-t) \cdot y \mid t \in [0,1]\} \subseteq M$$

Satz 7 (Gitterpunktsatz von Minkowski)**.** *Sei G ein Gitter und $M \subseteq \mathbb{R}^2$ konvex und punktsymmetrisch zum Ursprung. Gilt*

$$\mathrm{Vol}(M) > 4 \cdot \mathrm{Vol}(G),$$

so enthält M außer dem Ursprung einen weiteren Gitterpunkt.

Beweis. Sei v, w eine Gitterbasis von G und $P \coloneqq P(2v, 2w)$ viermal die Grundmasche von G. Somit gilt

$$\mathrm{Vol}(P) = 4\,\mathrm{Vol}(G) < \mathrm{Vol}(M).$$

Betrachte

$$\bigcup_{x \in 2G} (x + M) \cap P \subseteq P$$

Angenommen für alle $x, y \in 2G, x \neq y$ sind die Mengen $(x + M) \cap P$ und $(y + M) \cap P$ disjunkt. Damit gilt

$$\mathrm{Vol}(M) > \mathrm{Vol}(P) \geq \mathrm{Vol}(\bigcup_{x \in 2G} (x + M) \cap P) = \sum_{x \in 2G} \mathrm{Vol}((x + M) \cap P) = \mathrm{Vol}(M)$$

Widerspruch! Also existieren $x, y \in 2G, x \neq y$, sodass $x + M$ und $y + M$ einen gemeinsamen Punkt haben, es existieren also $a, b \in M$ mit $x + a = y + b$. Da M symmetrisch, liegt auch $-b \in M$. Wegen M konvex, gilt auch $\frac{a-b}{2} \in M$.
Es existieren $\lambda_v, \lambda_w, \mu_v, \mu_w \in \mathbb{Z}$, sodass $x = 2\lambda_v v + 2\lambda_w w, y = 2\mu_v v + 2\mu_w w$. Damit gilt

$$\frac{1}{2}(a - b) = \frac{1}{2}(y - x) = \frac{1}{2}(2\mu_v v + 2\mu_w w - 2\lambda_v v - 2\lambda_w w) = (\mu_v - \lambda_v)v + (\mu_w - \lambda_w)w \in G$$

Da $x \neq y$ ist dies nicht der Ursprung. ▲

Korollar 8 (kürzester Gittervektor)**.** *In einem Gitter G existiert ein Punkt P mit*

$$\|P\| \leq \sqrt{\frac{4}{\pi}\,\mathrm{Vol}(G)}.$$

Beweis: Sei $P \in G$ der Punkt mit minimaler Länge $\|P\|$[1]. Nach Definition enthält der randlose Kreis mit Radius $\|P\|$ um den Ursprung außer diesem keine Gitterpunkte. Nach dem Satz von Minkowski gilt also

$$\|P\|^2 \pi \leq 4\,\mathrm{Vol}(G)$$

▲

[1] Dieser existiert, da für $r \in \mathbb{R}$ groß genug im Kreis mit Radius r um den Ursprung mindestens ein, aber aufgrund der umgekehrten Dreiecksungleichung nur endlich viele Gitterpunkte liegen.

Zwei Quadrate Satz von Fermat

Satz 9 (Zwei Quadrate Satz)**.** *Eine ungerade Primzahl p kann genau dann als Summe von zwei Quadratzahlen dargestellt werden, wenn p bei der Division durch 4 Rest 1 hat.*

Beispiel.

$$2 = 1^2 + 1^2,\ 5 = 1^2 + 2^2,\ 13 = 2^2 + 3^2,\ 17 = 1^2 + 4^2, \dots$$

Beweis:
$p = 4n + 3\ \Rightarrow p$ nicht als Summe von zwei Quadraten darstellbar
Dies gilt sogar für alle Zahlen, die bei der Division durch 4 den Rest 3 haben, denn betrachtet man nur den Rest bei der Division durch 4, sind nur $0, 1$ Quadratzahlen. Insbesondere hat die Summe von zwei Quadratzahlen nicht Rest 3.

$p = 4n + 1\ \Rightarrow p$ ist als Summe von zwei Quadraten darstellbar
Für jede Primzahl obiger Form existiert eine Zahl $a \in \mathbb{N}$, sodass $a^2 + 1 \equiv 0 = p \cdot n$.[2]
Die Vektoren $\begin{pmatrix} p \\ 0 \end{pmatrix}, \begin{pmatrix} a \\ 1 \end{pmatrix}$ sind linear unabhängig, spannen also ein Gitter G auf. Es gilt

$$\mathrm{Vol}(G) = p$$

Sei K ein Kreis mit Radius $\sqrt{2p}$ um den Ursprung, dann gilt

$$\mathrm{Vol}(K) = 2\pi \cdot p > 4p = 4\,\mathrm{Vol}(G)$$

Nach dem Gitterpunktsatz von Minkowski existieren also $x, y \in \mathbb{Z}$ nicht beide 0, sodass:

$$Q \coloneqq x \cdot \begin{pmatrix} p \\ 0 \end{pmatrix} + y \cdot \begin{pmatrix} a \\ 1 \end{pmatrix} = \begin{pmatrix} x \cdot p + y \cdot a \\ y \end{pmatrix} \in K,$$

Es gilt

$$\|Q\|^2 = (xp + ya)^2 + y^2 = x^2p^2 + 2xypa + y^2(a^2 + 1) = (x^2p + 2xya)p + y^2(a^2 + 1),$$

Da $a^2 + 1 \equiv 0 \mod p$ ist dies ein Vielfaches von p. Da $Q \in K$ gilt außerdem

$$\|Q\|^2 < 2p.$$

Da $\mathbb{Q}$ nicht der Ursprung ist, folgt somit $\|Q\|^2 = p$. Damit erhält man

$$p = (xp + ya)^2 + y^2.$$

▲

Korollar 10 (Zwei Quadrate Satz)**.** *Eine natürliche Zahl ist genau dann als Summe zweier Quadrate darstellbar, wenn in ihrer Primfaktorzerlegung alle Primfaktoren der Form $4n + 3$ in gerader Potenz auftreten.*

Beispiel.

$2^3 \cdot 5 \cdot 13^2 \cdot 7^4 \cdot 11^2$ ist als Summe von zwei Quadraten darstellbar.

[2]Das folgt daraus, dass die multiplikative Gruppe des Körpers $\mathbb{Z}/p\mathbb{Z}$ zyklisch mit $4n$ Elementen ist, also ein Element der Ordnung 4 enthält.
Alternativ erhält man durch den kleinen Satz von Fermat für alle $x \in \mathbb{Z}/p\mathbb{Z}$ mit $p = 4n + 1$:
$0 = x^{4n} - 1 = (x^{2n} - 1)(x^{2n} + 1)\ \Rightarrow\ \exists y \in \mathbb{Z}/p\mathbb{Z} :\ y^8 + 1 = 0\ \Rightarrow\ (y^4)^2 = -1$