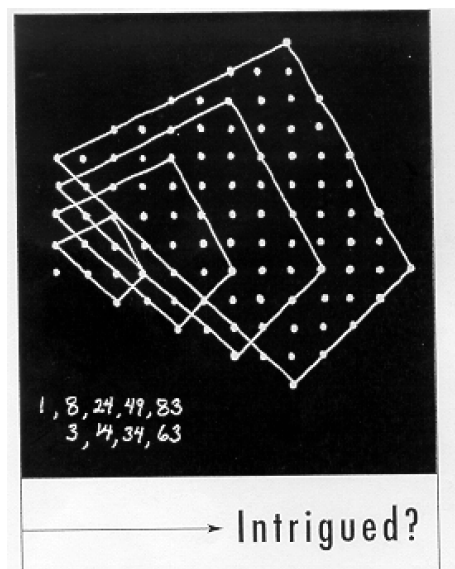


# Fastfood, quadratische Magie und Gitterpunkte

Mathematik-AG für Schülerinnen und Schüler  
Goethe-Universität, Sommer 2012



*Amir Dzambic* • *Elena Gerbig* • *Christian Haase*



# Inhaltsverzeichnis

|          |                                      |    |
|----------|--------------------------------------|----|
| <b>1</b> | <b>Gitterpunkte</b> .....            | 1  |
| 1.1      | Chicken McNuggets.....               | 1  |
| 1.2      | Quadratische Magie.....              | 2  |
| 1.3      | Polyeder .....                       | 2  |
| <b>2</b> | <b>Picks Formel</b> .....            | 5  |
| 2.1      | Vektorrechnung .....                 | 5  |
| 2.2      | $R = 3, I = 0$ .....                 | 7  |
| 2.3      | Vollständige Induktion .....         | 8  |
| 2.4      | Picks Formel.....                    | 9  |
| <b>3</b> | <b>Zwölf</b> .....                   | 11 |
| 3.1      | Polarität .....                      | 11 |
| 3.2      | Unimodulare Fächer .....             | 12 |
| 3.3      | Fächer-Unterteilungen .....          | 13 |
| 3.4      | Zusammenhang des Fächergraphen ..... | 13 |



# Kapitel 1

## Gitterpunkte

Wir werden uns in dieser Schüler-AG mit Gitterpunkten in Polytopen beschäftigen. In diesem ersten einführenden Kapitel wird erklärt, was die relevanten Objekte sind und warum wir uns für sie interessieren sollten. Das Kapitel dient hauptsächlich der Motivation. Es wird nicht alles haarklein definiert und es muss nicht alles in allen Details verstanden werden.

### 1.1 Chicken McNuggets

Eine „Restaurant“-Kette bietet frittierte Hühnchenstücke in 6er-, 9er- und 20er-Boxen an. Wieviele Möglichkeiten gibt es, genau 200 Hühnchenstücke zu bestellen?



$$\begin{aligned}
 Z = & z^{10} & , & n^{20}z & , & sn^6z^7 & , & s^2n^{12}z^4 \\
 & s^3n^{18}z & , & s^4n^4z^7 & , & s^5n^{10}z^4 & , & s^6n^{16}z \\
 & s^7n^2z^7 & , & s^8n^8z^4 & , & s^9n^{14}z & , & s^{10}z^7 \\
 & s^{11}n^6z^4 & , & s^{12}n^{12}z & , & s^{14}n^4z^4 & , & s^{15}n^{10}z \\
 & s^{17}n^2z^4 & , & s^{18}n^8z & , & s^{20}z^4 & , & s^{21}n^6z \\
 & s^{24}n^4z & , & s^{27}n^2z & , & s^{30}z & & 
 \end{aligned}$$

... dreiundzwanzig Möglichkeiten.

**1.1 Übung.** Man kann also nicht genau 7 Hühnchenstücke kaufen. Was ist die größte Zahl mit dieser Eigenschaft (die Frobeniuszahl)?

Auf dem Planeten Qkargogg gibt es Sparmenüs mit jeweils

12'223, 12'224, 36'674, 61'119, und 85'569

Hühnchenstücken. Wieviele Möglichkeiten gibt es, 89'643'482 zu bestellen?

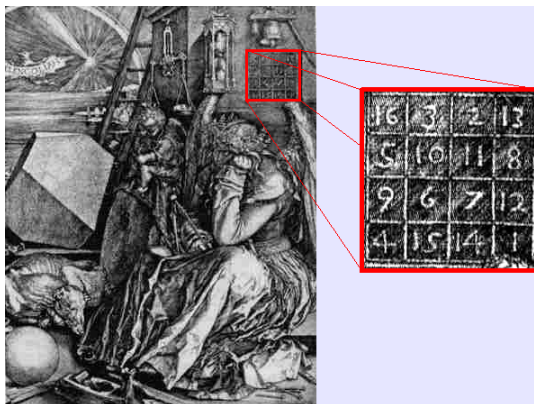
$$12223x_1 + 12224x_2 + 36674x_3 + 61119x_4 + 85569x_5 = 89643482$$

Wieviele NICHT-NEGATIVE, GANZZAHLIGE Lösungen?

März-2012

*Probleme dieser Bauart wurden schon zum Verschlüsseln von geheimen Nachrichten benutzt [Merkle, Hellman 1978]. Es war eines der ersten sogenannten public-key Kryptosysteme.*

### 1.2 Quadratische Magie



$$\begin{bmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{bmatrix}$$

|    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|
| 0  | 29 | 40 | 53 | 22 | 11 | 62 | 35 |
| 46 | 51 | 6  | 27 | 56 | 37 | 16 | 13 |
| 20 | 9  | 60 | 33 | 2  | 31 | 42 | 55 |
| 58 | 39 | 18 | 15 | 44 | 49 | 4  | 25 |
| 41 | 52 | 1  | 28 | 63 | 34 | 23 | 10 |
| 7  | 26 | 47 | 50 | 17 | 12 | 57 | 36 |
| 61 | 32 | 21 | 8  | 43 | 54 | 3  | 30 |
| 19 | 14 | 59 | 38 | 5  | 24 | 45 | 48 |

Abb. 1.1: Zwei magische Quadrate

Ein magisches Quadrat ist eine Matrix, bei der alle Zeilen-,Spalten- und Diagonalsummen denselben Wert — die magische Konstante — haben.

Für eine  $3 \times 3$ -Matrix übersetzt sich das in ein System linearer Gleichungen in neun Variablen.

$$\begin{bmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{bmatrix}$$

$$\begin{aligned} x_1 + x_2 + x_3 &= mc & x_4 + x_5 + x_6 &= mc & x_7 + x_8 + x_9 &= mc \\ x_1 + x_4 + x_7 &= mc & x_2 + x_5 + x_8 &= mc & x_3 + x_6 + x_9 &= mc \\ x_1 + x_5 + x_9 &= mc & x_3 + x_5 + x_7 &= mc & & \end{aligned}$$

Wieviele NICHT-NEGATIVE, GANZZAHLIGE Lösungen?

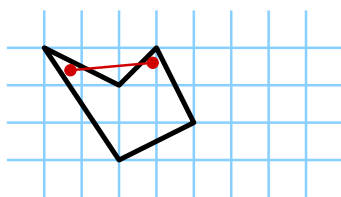


Abb. 1.2: Diese Figur ist nicht konvex: es gibt zwei Punkte, deren Verbindungstrecke nicht im Polytop liegt.

### 1.3 Polyeder

Ein Polyeder ist geometrisch als eine Figur beschrieben, die von endlich vielen ebenen Flächen begrenzt wird. Wir unterscheiden zwischen konvexen und nicht-konvexen Polyedern: Ein Polyeder (oder allgemeiner eine beliebige Teilmenge des Raums) heißt konvex, wenn die gesamte Verbindungstrecke zwischen je zwei Punkten des Polyeders ganz im Polyeder enthalten ist. Anschaulich heißt das, dass das Polyeder keine „Einbuchtungen“ besitzt. Desweiteren unterscheiden wir zwischen beschränkten und unbeschränkten Polyedern. Ein Polyeder ist beschränkt, wenn es in alle Richtungen geschlossen ist. Je zwei benachbarte begrenzende Flächen eines Polyeders (Seiten) schneiden sich in einer Strecke, die eine Kante des Polyeders definiert. In einem beschränkten Polyeder definieren sich schneidende Kanten eine Ecke. Jedes Polyeder hat nach Voraussetzung endlich viele Flächen, Kanten und Ecken. Ist übrigens das Polyeder beschränkt und konvex, dann gilt die folgende wichtige Beziehung zwischen der Anzahl der Flächen  $F$ , Kanten  $K$  und Ecken  $E$  – die sogenannte Eulersche Polyederformel:  $E - K + F = 2$  (Du darfst diese Formel an deinem

Lieblingpolyeder überprüfen, siehe etwa Abb. 1.3). Die einfachste Methode ein konvexes und beschränktes Polyeder zu konstruieren ist, die konvexe Hülle von endlich vielen Punkten (=Ecken des Polyeders) zu bilden. Die konvexe Hülle von endlich vielen Punkten  $p_1, \dots, p_n$  ist nach Definition die kleinste konvexe Menge, die alle diese Punkte enthält. Praktisch verbindet man alle Punkte miteinander durch Strecken. Das entstehende Gerüst definiert ein Polyeder. Die konvexe Hülle endlich vieler Punkte nennen wir ein Polytop.

Polyeder kann man nicht nur im dreidimensionalen Raum betrachten. Das zweidimensionale Analogon eines beschränkten Polyeders ist ein geschlossener Streckenzug. Es handelt sich dabei um eine Figur in der Ebene, die ausschließlich von Strecken begrenzt wird. Ein zweidimensionales Polytop, also die konvexe Hülle endlich vieler Punkte in der Ebene, ist ein Polygon.

**1.2 Übung.** Man beschreibe geometrisch die konvexe Hülle von drei Punkten in der Ebene und die konvexe Hülle von vier Punkten im Raum (man beachte auch die Lage der Punkte).

Um höherdimensionale Polyeder, die wir mit unserer Anschauung nicht mehr so gut fassen können, richtig beschreiben zu können, aber auch um interessante Eigenschaften ebener Polygone zu entdecken, ist eine weitere algebraische Beschreibung derselben sehr nützlich. Legt man in die Ebene ein Koordinatensystem, dann lässt sich jeder Punkt der Ebene als ein Vektor  $\begin{pmatrix} p \\ q \end{pmatrix}$  darstellen. Jede Gerade in der Ebene kann man durch eine lineare Gleichung der Form  $Ax + By = C$  beschreiben, wobei  $A, B, C$  feste reelle Zahlen und  $x, y$  Unbekannte sind. Die Lösungen der linearen Gleichung sind dann die Komponenten der Koordinatenvektoren  $\begin{pmatrix} x \\ y \end{pmatrix}$ , die auf der Geraden liegen.

**1.3 Übung.** Man bestimme die Gleichung  $Ax + By = C$  der Geraden, die durch die Punkte

- (1)  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$  und  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$   
 (2)  $\begin{pmatrix} 3 \\ 0 \end{pmatrix}$  und  $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$

geht.

Die Gleichungen  $x = 0$ ,  $x = 1$ ,  $y = 0$ ,  $y = 1$  beschreiben die Geraden, die ein Polygon – das Einheitsquadrat – begrenzen. Das Quadrat selbst ist durch die Liste von Ungleichungen  $x \geq 0$ ,  $x \leq 1$ ,  $y \geq 0$ ,  $y \leq 1$  gegeben. Im Allgemeinen ist also ein Polygon oder ein zweidimensionales Polyeder durch eine Reihe von linearen Ungleichungen gegeben. Bei dreidimensionalen Polyedern ist das nicht anders. Ebenen im dreidimensionalen Raum sind durch lineare Gleichungen der Form  $Ax + By + Cz = D$  beschrieben. Eine endliche Liste von Ungleichungen des Typs  $Ax + By + Cz \leq D$  definieren ein dreidimensionales Polyeder. Dabei ist zu beachten, dass jede einzelne Gleichung  $Ax + By + Cz = D$  genau eine Seite des Polyeders beschreibt, und dass die Punkte (besser gesagt ihre Koordinaten) auf den Kanten zwei solcher Gleichungen erfüllen. Entsprechend sind die Ecken Punkte des Polyeders, die mehr als zwei Gleichungen aus der Liste erfüllen.

**1.4 Übung.** Man gebe die Ungleichungen an, die einen Würfel beschreiben. Wie sind die Kanten und die Ecken des Würfels beschrieben?

Mit Hilfe von linearen Ungleichungen in noch mehr Variablen lassen sich Polyeder und Polytope in beliebiger Dimension definieren. Wir sagen einfach: Die Lösungsmenge endlich vieler linearer Ungleichungen ist ein Polyeder. Die folgende Aussage gilt in allen Dimensionen:

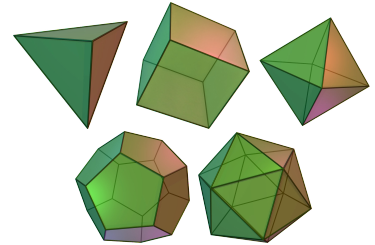


Abb. 1.3: Fünf Polytope

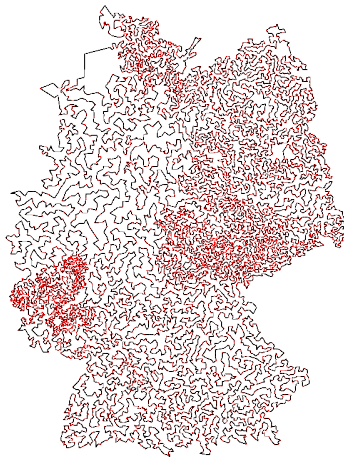


Abb. 1.4: Die kürzeste Rundtour durch 15'112 deutsche Städte wurde als Gitterpunkt in einem 114'163'604-dimensionalen Polytop gefunden. Von [www.tsp.gatech.edu](http://www.tsp.gatech.edu)

### 1.5 Theorem (Minkowski 1897, Weyl 1935).

$$\text{beschränktes Polyeder} = \text{Polytop}$$

Ein Polytop, bei dem alle Ecken nur ganzzahlige Koordinaten haben, heißt Gitterpolytop.

Das Problem, nicht-negative ganzzahlige Lösungen für ein System linearer Gleichungen — also Gitterpunkte in Polytopen — zu finden, ist das sogenannte Problem der ganzzahligen Optimierung. Es ist heutzutage eines der am häufigsten auftauchenden mathematischen Probleme in der Praxis.

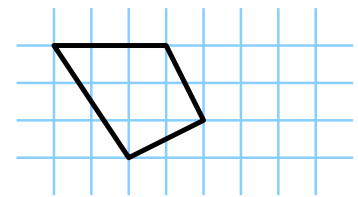


## Kapitel 2

### Picks Formel

Von nun an wollen wir uns auf den Fall zweidimensionaler Polytope — Polygone — beschränken. Ziel dieses Kapitels ist es, eine berühmte Formel von Georg Alexander Pick für die Fläche von Gitterpolygonen zu beweisen.

**2.1 Übung.** Zeichne auf Karopapier einige Gitterpolygone. Bestimme ihre Fläche  $A$ , die Anzahl  $I$  der inneren Gitterpunkte sowie die Anzahl  $R$  der Randgitterpunkte. Erstelle eine Wertetabelle. Findest Du einen Zusammenhang zwischen diesen drei Größen?



|   |   |   |
|---|---|---|
| A | I | R |
| 7 | 5 | 6 |

Abb. 2.1: Ein Gitterpolygon und sein Eintrag in der Wertetabelle

### 2.1 Vektorrechnung

Um Picks Formel für alle Gitterpolygone zu beweisen, behandeln wir zunächst den Spezialfall  $I = 0$ ,  $R = 3$ . Dafür wiederum brauchen wir eine Formel für die Fläche eines Parallelogramms. Diese Formel kommt in natürlicher Weise in der Vektorrechnung vor. Wir wollen in einem Schnelldurchlauf einige grundlegenden Konzepte, die hinter den Gitterpolygonen stecken, vorstellen. Das kartesische Koordinatensystem ist uns aus der Schule bekannt. Dort zeichnet man zwei senkrecht aufeinander stehende Geraden aus (Koordinatenachsen) und stellt jeden Punkt der Ebene als einen Vektor  $\begin{pmatrix} p \\ q \end{pmatrix}$  dar. Mit anderen Worten ist der Vektor  $\begin{pmatrix} p \\ q \end{pmatrix}$  eine „lineare Kombination“  $p\begin{pmatrix} 1 \\ 0 \end{pmatrix} + q\begin{pmatrix} 0 \\ 1 \end{pmatrix}$  der „Basisvektoren“  $e_1 := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  und  $e_2 := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ . Dabei gelten die Rechenregeln

$$p \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} px \\ py \end{pmatrix}$$

$$\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x + x' \\ y + y' \end{pmatrix}$$

In dieser Darstellung sind die Koordinatenachsen einfach die Mengen der Vielfachen der Basisvektoren (die x-Achse etwa entspricht  $\{te_1 \mid t \text{ reelle Zahl}\}$ ). Allgemein definiert in gleicher Weise ein beliebiger Vektor eine Gerade durch den Ursprung  $\mathbf{0} := \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ . Man beachte aber, dass die Darstellung der Punkte der Ebene von der Wahl der Basisvektoren  $e_1$  und  $e_2$  abhängt. Die ganzzahligen Linearkombinationen  $pe_1 + qe_2$  ( $p, q$  ganze Zahlen) definieren ein ebenes Gitter  $\mathbb{Z}^2$ . Gleichzeitig ist die konvexe Hülle von  $\mathbf{0}$ ,  $e_1$  und  $e_2$  ein ebenes Gitterpolygon, ein Dreieck, welches nur am Rand (drei) Gitterpunkte enthält.

Allgemeiner können wir das gleiche Spiel mit zwei beliebigen Vektoren  $v = \begin{pmatrix} p \\ q \end{pmatrix}$  und  $w = \begin{pmatrix} r \\ s \end{pmatrix}$ , die nicht auf einer Geraden durch den Ursprung liegen,

spielen. Wir können jeden Punkt der Ebene als Linearkombination  $av + bw$  mit gewissen reellen Zahlen  $a, b$  schreiben. Diese Koeffizienten  $a, b$  sind die „Koordinaten“ bezüglich der neuen Basis  $v$  und  $w$ .

**2.2 Übung.** Drücke die beiden Vektoren  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$  und  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$  als Linearkombination  $av + bw$  der folgenden Vektoren aus

- (1)  $v = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$  und  $w = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$ ,
- (2)  $v = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$  und  $w = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ ,
- (3)  $v = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$  und  $w = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$ ,
- (4)  $v = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$  und  $w = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$ .

Beachte: Manchmal sind die „Koordinaten“  $a, b$  auch ganze Zahlen und manchmal nicht. Kannst du auch einen Grund dafür finden? (schwer!)

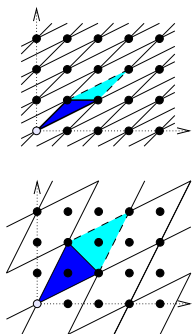


Abb. 2.2: Pflasterungen der Ebene

Nehmen wir an, dass  $p, q, r, s$  allesamt ganze Zahlen sind. Dann ist die Menge der ganzzahligen Linearkombinationen von  $v$  und  $w$ , also das von  $v$  und  $w$  aufgespannte Gitter, ein Teilgitter des „Standardgitters“  $\mathbb{Z}^2$ , das von  $e_1$  und  $e_2$  erzeugt wird. Zu gegebenen zwei ganzzahligen Vektoren  $v = \begin{pmatrix} p \\ q \end{pmatrix}$  und  $w = \begin{pmatrix} r \\ s \end{pmatrix}$  ist neben der konvexen Hülle von  $0, v$  und  $w$  noch ein Gitterpolygon von zentraler Bedeutung. Das von  $v$  und  $w$  aufgespannte Parallelogramm, also die konvexe Hülle von  $0, v, w$  und  $v + w$ , heißt auch die Grundmasche des zugehörigen Gitters.

**2.3 Übung.** Bestimme das Gitter sowie das zugehörige Parallelogramm, das von den folgenden Vektoren aufgespannt wird

- (1)  $v = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$  und  $w = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$ ,
- (2)  $v = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$  und  $w = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ ,
- (3)  $v = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$  und  $w = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$ ,
- (4)  $v = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$  und  $w = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$ .

Untersuche die Unterschiede und Gemeinsamkeiten zwischen den verschiedenen Gitterpolygonen und zugehörigen Gittern.

Eine wichtige Eigenschaft dieser Parallelogramme ist die Folgende: Verschiebt man das von  $v$  und  $w$  erzeugte Parallelogramm in ganzzahligen Schritten in Richtung von  $v$  und  $w$ , dann pflastert man die gesamte Ebene mit Überlappungen nur am Rand. Die Fläche der Grundmasche ist ebenfalls eine zentrale Größe.

**2.4 Proposition.** Die Fläche  $A(p, q, r, s)$  des von den Vektoren  $\begin{pmatrix} p \\ q \end{pmatrix}$  und  $\begin{pmatrix} r \\ s \end{pmatrix}$  aufgespannten Parallelogramms beträgt  $|ps - rq|$ .

*Beweis.* Durch Scheren sehen wir, dass für jede Zahl  $t$  das Parallelogramm, das von den Vektoren  $v$  und  $w$  aufgespannt wird, die gleiche Fläche hat, wie das Parallelogramm, das von den Vektoren  $v$  und  $tv + w$  aufgespannt wird: sie haben beide die gleiche Grundseite  $[0, v]$  und die gleiche Höhe. Es gelten also die folgenden Rechenregeln.

$$A(tp, tq, r, s) = A(p, q, tr, ts) = |t|A(p, q, r, s)$$

$$A(p, q, r, s) = A(p, q, r + p, s + q) = A(p + r, q + s, r, s)$$

Falls  $p = q = 0$  ist  $A(p, q, r, s) = A(0, 0, r, s) = 0 = |ps - qr|$ .  
 Falls nun  $p \neq 0$  (oder  $q \neq 0$ ) können wir wie folgt folgern.

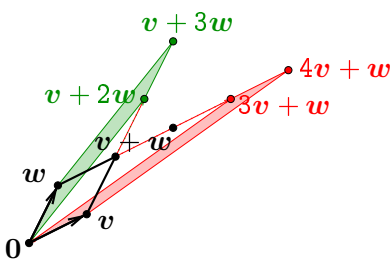


Abb. 2.3:  $A(v, w) = A(v, 3v + w) = A(v + 2w, w)$

$R = 3, I = 0$

7

$$A(p, q, r, s) = |p|A(1, q/p, r, s) = |p|A(1, q/p, 0, s - qr/p)$$

Wenn außerdem  $ps - qr \neq 0$ , folgern wir weiter

$$= |p|A(1, 0, 0, s - qr/p) = |ps - qr|A(1, 0, 0, 1) = |ps - qr|.$$

Sollte aber  $ps - qr = 0$  sein, wäre

$$A(p, q, r, s) = |p|A(1, q/p, 0, 0) = 0 = |ps - qr|.$$

□

Eine solche Formel gibt es in jeder Dimension. Sie heißt die „Determinante“ und wird im ersten Semester in der Vorlesung Lineare Algebra behandelt.

Als Nächstes brauchen wir das folgende Lemma (=Hilfssatz). Auch diese Eigenschaft — der Determinantenmultiplikationssatz — überträgt sich in allgemeine Dimension.

**2.5 Lemma.** Wenn  $\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} aa'+cb' & ac'+cd' \\ ba'+db' & bc'+dd' \end{pmatrix}$ , dann ist

$$A(p, q, r, s) = A(a, b, c, d) \cdot A(a', b', c', d').$$

*Beweis.* Nachrechnen.

□

## 2.2 $R = 3, I = 0$

Mithilfe von Lemma 2.5 können wir nun Picks Formel im Fall  $R = 3, I = 0$  beweisen.

**2.6 Proposition.** Ein Dreieck, dessen Gitterpunkte genau die Ecken sind, hat Fläche  $1/2$ .

*Beweis.* Die Fläche des Dreiecks mit Ecken  $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ ,  $\begin{pmatrix} p \\ q \end{pmatrix}$ ,  $\begin{pmatrix} r \\ s \end{pmatrix}$  ist die Hälfte von  $A(p, q, r, s)$ .

Die Verschiebungen um Vielfache von  $\begin{pmatrix} p \\ q \end{pmatrix}$  und  $\begin{pmatrix} r \\ s \end{pmatrix}$  pflastern die Ebene.

Nachdem es außer den Ecken keine Gitterpunkte im Parallelogramm gibt, lassen sich alle Gitterpunkte in der Form  $n\begin{pmatrix} p \\ q \end{pmatrix} + m\begin{pmatrix} r \\ s \end{pmatrix}$  mit ganzen Zahlen  $m$  und  $n$  schreiben. Insbesondere gibt es ganze Zahlen  $a, b, c, d$ , so dass  $\begin{pmatrix} 1 \\ 0 \end{pmatrix} = a\begin{pmatrix} p \\ q \end{pmatrix} + b\begin{pmatrix} r \\ s \end{pmatrix}$  und  $\begin{pmatrix} 0 \\ 1 \end{pmatrix} = c\begin{pmatrix} p \\ q \end{pmatrix} + d\begin{pmatrix} r \\ s \end{pmatrix}$ .

Damit können wir Lemma 2.5 anwenden, so dass  $1 = A(1, 0, 0, 1) = A(p, q, r, s) \cdot A(a, b, c, d)$ . Nun sind aber beide Faktoren positive ganze Zahlen. Sie müssen also beide 1 sein.

□

**2.7 Anmerkung.** Dreiecke, wie wir sie eben untersucht haben, heißen unimodular. Wir haben mit unserem Beweis gezeigt, dass sich jeder Gitterpunkt als Summe von ganzzahligen Vielfachen der Ecken eines beliebigen unimodularen Dreiecks schreiben läßt.

**2.8 Beispiel.** Das Analogon zu Proposition 2.6 ist falsch in Dimension 3. John Reeve hat 1957 Tetraeder beschrieben, die außer den Ecken  $\mathbf{0}$ ,  $(1, 0, 0)^t$ ,  $(0, 1, 0)^t$  und  $(1, 1, n)^t$  keine weiteren Gitterpunkte enthalten, deren Volumen  $n/6$  aber beliebig groß wird.

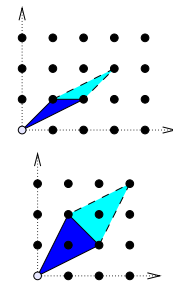


Abb. 2.4: Ein Parallelogramm ohne und eines mit weiteren Gitterpunkten

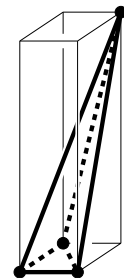


Abb. 2.5: Reeves Tetraeder enthalten außer den Ecken keine Gitterpunkte, haben aber beliebig großes Volumen.

## 2.3 Vollständige Induktion

Wie schon gesagt, wollen wir die allgemeine Aussage des Satzes von Pick aus der Richtigkeit der Aussage für den Fall  $I = 0$  und  $R = 3$  (das ist gerade die Aussage der Proposition 2.6) herleiten. Diese Herleitung folgt einem allgemeinen mathematischen Prinzip – dem sogenannten Prinzip der vollständigen Induktion. Möchten wir eine Aussage  $\mathcal{A}(n)$  über alle natürlichen Zahlen beweisen (Picks Satz ist in der Tat eine solche Aussage, die eine Beziehung zwischen den natürlichen Zahlen  $A, I, R$  herstellt), dann genügt es nach dem Prinzip der vollständigen Induktion folgendermaßen vorzugehen:

- (1) Man beweise, dass die Aussage  $\mathcal{A}(n_0)$  für eine kleinste natürliche Zahl  $n_0$  gilt (Induktionsanfang).
- (2) Man nehme an, dass die Aussage  $\mathcal{A}(k)$  für alle natürlichen Zahlen  $n_0 \leq k < n$  mit  $n$  beliebig gilt (Induktionsvoraussetzung) und folgere daraus, dass auch  $\mathcal{A}(n)$  gilt (Induktionsschluss).

Betrachten wir ein einfaches Beispiel für die Anwendung des Induktionsprinzips.

*2.9 Beispiel.* Zu beweisen ist die folgende Aussage, die für alle natürlichen Zahlen  $n \geq 1$  gelten soll:

$$1 + 2 + \dots + n = \frac{n(n+1)}{2}.$$

Für  $n = 1$  stimmt die Aussage offensichtlich, denn  $1 = \frac{1 \cdot 2}{2}$ . Das ist der Induktionsanfang. Jetzt nehmen wir an, dass für jede beliebige natürliche Zahl  $k < n$  tatsächlich gilt  $1 + 2 + \dots + k = \frac{k(k+1)}{2}$  (Induktionsvoraussetzung). Wir müssen nun zeigen, dass dann auch  $1 + 2 + \dots + n = \frac{n(n+1)}{2}$  gilt. Wir nutzen nun skrupellos die Induktionsvoraussetzung aus, nach der gilt  $1 + 2 + \dots + (n-1) = \frac{(n-1)n}{2}$  (wir setzen  $k = n-1$  ein). Es gilt

$$1 + 2 + \dots + n = [1 + 2 + \dots + (n-1)] + n \stackrel{(*)}{=} \frac{(n-1)n}{2} + n$$

((\*) nach Induktionsvoraussetzung), also

$$1 + 2 + \dots + n = \frac{(n-1)n}{2} + n = \frac{n^2 - n + 2n}{2} = \frac{n^2 + n}{2} = \frac{n(n+1)}{2}$$

Damit sind wir fertig. □

Es ist das Wesen und die Stärke der vollständigen Induktion, dass man die Gültigkeit der Aussage  $\mathcal{A}(n-1)$  wirklich skrupellos, ohne sich Gedanken zu machen, voraussetzen darf, um die Aussage  $\mathcal{A}(n)$  zu beweisen. (Aber bitte nicht den Induktionsanfang vergessen!) Das üben wir jetzt nochmal.

**2.10 Übung.** Man beweise mit Hilfe des Induktionsprinzips die folgenden Aussagen:

- (1) Für alle natürlichen Zahlen  $n \geq 3$  gilt  $2n + 1 \leq 2^n$ .
- (2) Ein ebenes beschränktes und konvexes  $n$ -Eck ( $n$ -gon) hat genau  $\frac{n(n-3)}{2}$  Diagonalen.

## 2.4 Picks Formel

Nachdem wir nun Meister dieser Beweistechnik sind, können wir schließlich und endlich den allgemeinen Fall von Picks Satz auf unimodulare Dreiecke zurückführen.

**2.11 Theorem (Pick 1899).** *Sei  $P$  ein Gitterpolygon mit Fläche  $A$  und mit  $I$  Gitterpunkten im Inneren und  $R$  auf dem Rand. Dann ist*

$$A = I + \frac{R}{2} - 1.$$

*Beweis.* Wir führen den Beweis per Induktion über  $n = R + I$  (die Aussage des Pickschen Satzes hängt jetzt formal nur von einer natürlichen Zahl ab). Sei  $P$  ein Gitterpolygon. Wenn  $I = 0$ ,  $R = 3$  ist, haben wir schon gezeigt, dass  $A = 1/2 = I + \frac{R}{2} - 1$  sein muss.

Wenn  $R + I > 3$ , also  $I > 0$  oder  $R > 3$  ist, können wir  $P$  in zwei kleinere Gitterpolygone zerschneiden:  $P = P' \cup P''$ , so dass  $P' \cap P''$  ein Streckenzug ist, der  $k$  Gitterpunkte enthält. Dann ist nach Induktionsvoraussetzung  $A' = I' + \frac{R'}{2} - 1$  und  $A'' = I'' + \frac{R''}{2} - 1$ .

Die Zerlegung zeigt uns  $A = A' + A''$ ,  $R = R' + R'' - 2k + 2$  und  $I = I' + I'' + k - 2$ . Wenn man diese Formeln addiert, erhält man wie gewünscht  $A = I + \frac{R}{2} - 1$ .  $\square$

Als erste und unmittelbare Anwendung von Pick's Formel können wir den zweidimensionalen Fall eines Satzes von Eugène Ehrhart über die Anzahl der Gitterpunkte in Streckungen von Gitterpolytopen beweisen.

**2.12 Theorem (Ehrhart 1962, Macdonald 1971).** *Sei  $P$  ein Gitterpolygon. Dann gibt es ein Polynom  $f(k)$ , so dass für positive ganze Zahlen  $k$*

$$|kP \cap \mathbb{Z}^2| = f(k) \quad \text{und} \quad |\text{int}(kP) \cap \mathbb{Z}^2| = f(-k)$$

*Beweis.* Für  $k \in \mathbb{Z}_{>0}$  bezeichne mit  $A(k)$ ,  $I(k)$ ,  $R(k)$  die Fläche, die Anzahl der inneren Gitterpunkte respektive die Anzahl der Randgitterpunkte von  $kP$ . Dann ist  $A(k) = Ak^2$  (das gilt für jede Streckung einer zweidimensionalen Figur) und  $R(k) = Rk$ . Dann besagt Picks Formel für  $kP$ , dass

$$I(k) = A \cdot k^2 - \frac{R}{2} \cdot k + 1$$

also

$$R(k) + I(k) = A \cdot k^2 + \frac{R}{2} \cdot k + 1.$$

$\square$

Die entsprechenden Aussagen in allgemeiner Dimension gehen auf Eugène Ehrhart zurück. Das Polynom, das die Anzahl der Gitterpunkte in  $kP$  berechnet, heißt deshalb auch Ehrhart-Polynom. Es ist Gegenstand intensiver Forschung. Eugène Ehrhart war Gymnasiallehrer und, was mathematische Forschung angeht, Autodidakt. Er hat im Alter von 40 Jahren seine erste wissenschaftliche Arbeit publiziert und im Alter von 60 Jahren promoviert — ein echter Spätstarter.

Wir schließen diesen Abschnitt mit einer offenen Forschungsfrage.

**2.13 Frage.** Gibt es ein 3-dimensionales Gitterpolytop mit 2 inneren Gitterpunkten und Volumen  $> 18$ ? oder mit  $> 53$  Randgitterpunkten?

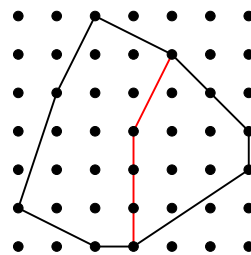


Abb. 2.6: Zerschnittenes  $P$



Abb. 2.7: Eugène Ehrhart by Eugène Ehrhart



## Kapitel 3

### Zwölf

In diesem Kapitel beweisen wir eine eigentümliche Eigenschaft von Gitterpolygonen mit einem inneren Gitterpunkt. Um diese Eigenschaft zu formulieren müssen wir das Polare eines solchen Polygons definieren.

#### 3.1 Polarität

Polarität ist eine Operation, die aus einem Gitterpolygon  $P$  mit genau einem inneren Gitterpunkt ein anderes Gitterpolygon  $P^\circ$  macht, das auch wieder genau einen inneren Gitterpunkt hat. Um nicht immer „Gitterpolygon mit genau einem inneren Gitterpunkt  $\mathbf{0}$ “ schreiben zu müssen, nennen wir solche Polygone ab jetzt reflexiv.

Sei also  $P$  reflexives Polygon. Dann sind die Randgitterpunkte gegen den Uhrzeigersinn zyklisch geordnet:  $v_1, \dots, v_r$ . Dann definieren wir das polare Polygon  $P^\circ$  als die konvexe Hülle der Vektoren  $v_2 - v_1, v_3 - v_2, \dots, v_r - v_{r-1}, v_1 - v_r$ .

Damit gibt es zu jedem Segment  $[v_{i-1}, v_i]$  auf dem Rand von  $P$  einen „polaren“ Randgitterpunkt  $w_i := v_i - v_{i-1}$  von  $P^\circ$  (mit der Konvention  $v_{r+1} = v_1$  und analog  $w_{r+1} = w_1$ ). Umgekehrt gibt es für jedes Segment  $[w_{i+1}, w_i]$  auf dem Rand von  $P^\circ$  einen polaren Randgitterpunkt  $v_i$  von  $P$ .

**3.1 Proposition.** *Wenn  $P$  reflexiv ist, dann ist auch  $P^\circ$  reflexiv.*

*Beweis.* Wenn  $v_{i-1} = \begin{pmatrix} p \\ q \end{pmatrix}$  und  $v_i = \begin{pmatrix} r \\ s \end{pmatrix}$ , dann ist die Gleichung der Geraden durch  $v_{i-1}$  und  $v_i$  durch die Gleichung  $(s - q)x + (p - r)y = ps - rq = 1$  gegeben. Dabei haben wir für die zweite Gleichheit benutzt, dass das Dreieck  $\text{conv}(\mathbf{0}, v_{i-1}, v_i)$  keine weiteren Gitterpunkte enthält, dass also nach Picks Formel und Proposition 2.4  $A(v_{i-1}, v_i) = ps - rq = 1$  ist.

Es gilt also  $(s - q)x + (p - r)y \leq 1$  für jeden Punkt  $\begin{pmatrix} x \\ y \end{pmatrix}$  in  $P$ . Wenn man beachtet, dass  $w_i = \begin{pmatrix} r-p \\ s-q \end{pmatrix}$ , kann man diese Ungleichung als Ungleichung für  $P^\circ$  uminterpretieren:  $-ya + xb \leq 1$  für alle  $\begin{pmatrix} a \\ b \end{pmatrix} \in P^\circ$  und alle  $\begin{pmatrix} x \\ y \end{pmatrix} \in P$ .

Wenn dabei  $\begin{pmatrix} x \\ y \end{pmatrix} = v_i$  und  $\begin{pmatrix} a \\ b \end{pmatrix}$  ein innerer Gitterpunkt von  $P^\circ$  ist, muss die linke Seite eine ganze Zahl  $< 1$  und deshalb  $\leq 0$  sein. Damit ist dann aber  $-ya + xb \leq 0$  für alle  $\begin{pmatrix} x \\ y \end{pmatrix} \in P$ . Nachdem  $P$  eine Umgebung von  $\mathbf{0}$  ist, kann nur  $\begin{pmatrix} a \\ b \end{pmatrix} = \mathbf{0}$  diese Bedingungen erfüllen.  $\square$

**3.2 Übung.** Sei  $P$  reflexiv. Überzeuge Dich, dass  $P^{\circ\circ} = -P$ .

**3.3 Übung.** Konstruiere möglichst viele Paare zueinander polarer reflexiver Gitterpolygone. Zähle ihre Randgitterpunkte; fällt Dir etwas auf?

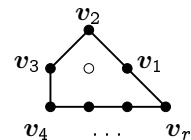


Abb. 3.1: Zyklisch geordnete Randgitterpunkte

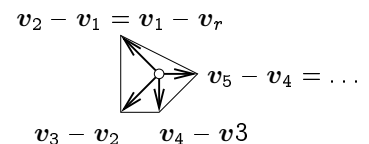
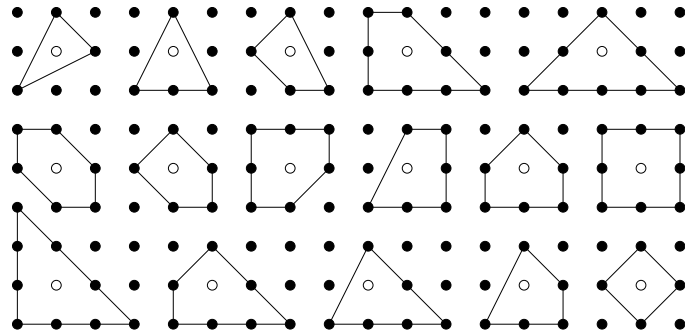


Abb. 3.2: Das polare Polygon  $P^\circ$

*Polarität von Polytopen funktioniert auch in höheren Dimensionen. Allgemein nennt man dann Gitterpolytope  $P$ , für die  $P^\circ$  wieder ein Gitterpolytop ist reflexiv. Reflexive Polytope spielen in der algebraischen Geometrie und in der theoretischen Physik eine Rolle.*



### 3.2 Unimodulare Fächer

Am Ende des letzten Abschnitts ist uns aufgefallen, dass für ein Gitterpolygon  $P$  mit genau einem inneren Gitterpunkt  $P$  und  $P^\circ$  zusammen immer 12 Randgitterpunkte haben. Dass das tatsächlich immer so sein muss, wollen wir im nächsten Abschnitt beweisen. Für den Beweis werden wir in diesem Abschnitt die Aussage auf sogenannte unimodulare Fächer verallgemeinern.

Ein Strahl  $S$  ist eine Halbgerade in der Ebene mit Endpunkt  $0$ , die von einem Gittervektor  $v$  erzeugt wird:  $S = \{sv : s \geq 0\}$ . Zwei Gittervektoren  $v, w$ , die nicht kollinear sind spannen einen Kegel  $K = \{sv + tw : s, t \geq 0\}$  auf. Der Kegel  $K$  heißt unimodular, wenn  $v$  und  $w$  so gewählt werden können, dass das Dreieck  $\text{conv}(0, v, w)$  keine weiteren Gitterpunkte enthält. Wenn wir von Erzeugern eines Strahls oder eines Kegels sprechen, meinen wir immer den kürzesten Gittervektor auf dem Strahl, beziehungsweise die beiden kürzesten Gittervektoren auf den Strahlen des Kegels.

Ein Fächer  $F$  ist eine Zerlegung der Ebene in solche Kegel. Wenn alle Kegel unimodular sind, heißt auch  $F$  unimodular. Solche unimodularen Fächer erhält man zum Beispiel, wenn man einen Strahl durch jeden Randgitterpunkt eines reflexiven Polygons zeichnet.

Wir kommen nun zur ersten wichtigen Eigenschaft unimodularer Fächer.

**3.4 Lemma.** *Jeder Strahl  $S$  mit Erzeuger  $v$  in einem unimodularen Fächer  $F$  liegt in genau zwei Kegeln  $K = \text{cone}(v, w)$  und  $K' = \text{cone}(v, w')$  in  $F$ .*

*In dieser Situation gibt es eine eindeutig bestimmte ganze Zahl  $f_F(S)$ , so dass*

$$w + w' = f_F(S)v.$$

*Beweis.* Die beiden Dreiecke  $\text{conv}(0, v, w)$  und  $\text{conv}(0, v, w')$  haben nach Picks Formel die gleiche Fläche. Sie haben auch beide die gleiche Grundseite  $[0, v]$ . Also müssen sie auch die gleiche Höhe haben. Nachdem  $w$  und  $w'$  auf verschiedenen Seiten von  $S$  liegen, hat ihre Summe die „Höhe“ Null.  $\square$

**3.5 Übung.** Bestimme für den Fächer eines reflexiven Polygons alle Parameter  $f_F(S)$ . Zeichne dazu das Polare Polygon. Fällt Dir etwas auf?

Im Folgenden messen wir die Länge von Strecken immer in Bezug auf das Gitter. Das heißt, die Länge einer Strecke ist für uns eins weniger als die Anzahl der Gitterpunkte auf der Strecke.

**3.6 Lemma.** *Sei  $P$  ein reflexives Polygon, und seien  $w, v, w'$  aufeinander folgende Gitterpunkte auf dem Rand von  $P$  mit  $w + w' = fv$ .*

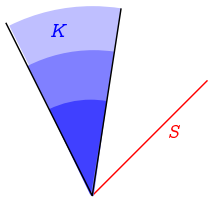


Abb. 3.3: Ein Strahl und ein Kegel

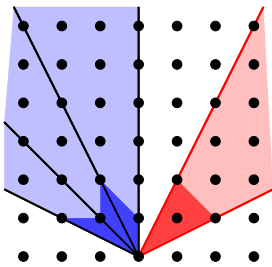


Abb. 3.4: Einige unimodulare Kegel und ein nicht-unimodularer Kegel

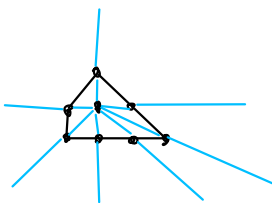


Abb. 3.5: Der Fächer eines reflexiven Polygons

4-Apr-2012

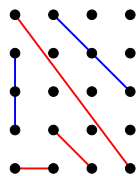


Abb. 3.6: Strecken der Länge eins und der Länge zwei



Wenn  $v$  eine Ecke von  $P$  ist, dann hat die zu  $v$  polare Kante von  $P^\circ$  die Länge  $2 - f$ . (Wenn  $v$  keine Ecke ist, dann ist  $f = 2$ .)

*Beweis.* Per Definition läuft die zu  $v$  polare Kante von  $v - w$  nach  $w' - v$ . Die Differenz der beiden Endpunkte ist also

$$(v - w) - (w' - v) = 2v - (w + w') = (2 - f_F)v .$$

□

Im Lichte dieses Lemmas können wir jetzt die angekündigte Verallgemeinerung formulieren.

**3.7 Theorem.** Sei  $F$  ein unimodularer Fächer. Dann ist

$$\sum_{S \text{ Strahl von } F} (3 - f_F(S)) = 12. \quad (3.2.1)$$

### 3.3 Fächer-Unterteilungen

Wir werden Theorem 3.7 beweisen, indem wir zwischen Fächern hin und her laufen. In diesem Abschnitt definieren wir die Schritte, elementare Verfeinerungen und elementare Vergrößerungen, mit denen wir von einem Fächer zum nächsten kommen. Dann überzeugen wir uns noch, dass die linke Seite von (3.2.1) bei diesen Schritten konstant bleibt. Im nächsten Abschnitt zeigen wir dann, dass man tatsächlich von jedem unimodularen Fächer zu jedem anderen mithilfe einer Folge solcher Schritte gelangen kann. Aber eins nach dem anderen.

Sei  $F$  ein unimodularer Fächer, und sei  $K$  ein Kegel in  $F$  mit Erzeugern  $w, w'$ . Setze  $v := w + w'$  und  $S := \text{cone}(v)$ . Dann erhalten wir einen neuen Fächer  $\text{pull}(F; S)$  indem wir den Kegel  $K$  aus  $F$  entfernen und durch die beiden Kegel  $\text{cone}(w, v)$  und  $\text{cone}(v, w')$  ersetzt.

Wir sagen, dass der Fächer  $\text{pull}(F; S)$  durch eine elementare Verfeinerung aus  $F$  hervorgeht. Umgekehrt geht  $F$  aus  $\text{pull}(F; S)$  durch eine elementare Vergrößerung hervor. Die definierende Eigenschaft einer solchen elementaren Verfeinerung ist die Tatsache, dass der neue Strahl  $S$  den Parameter  $f_F(S) = 1$  hat. Soll heißen: wenn ein Strahl in einem unimodularen Fächer den Parameter 1 hat, dann ist dieser Fächer die elementare Verfeinerung eines größeren Fächers.

**3.8 Übung.** Sei  $F' = \text{pull}(F; S)$  elementare Verfeinerung des unimodularen Fächers  $F$ . Zeige, dass

$$\sum_{S' \text{ Strahl von } F'} (3 - f_{F'}(S')) = \sum_{S \text{ Strahl von } F} (3 - f_F(S)).$$

### 3.4 Zusammenhang des Fächergraphen

In diesem Abschnitt wollen wir zeigen, dass je zwei unimodulare Fächer durch eine Abfolge von elementaren Verfeinerung und elementaren Vergrößerungen auseinander hervorgehen und damit den Beweis von Theorem 3.7 abschließen.

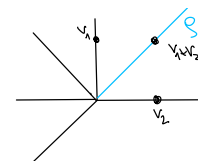


Abb. 3.7: Eine elementare Verfeinerung

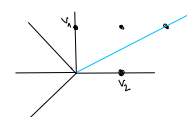


Abb. 3.8: Keine elementare Verfeinerung

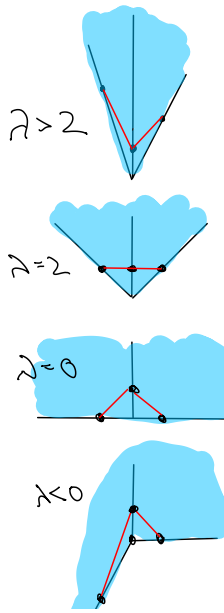


Abb. 3.9: Verschiedene  $f_F$ 's

proof missing

Auch die Aussage von Lemma 3.11 gilt in beliebiger Dimension, ist aber erheblich aufwendiger zu beweisen.

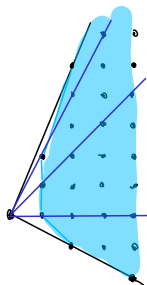


Abb. 3.10: Unimodulare Unterteilung eines Kegels

**3.9 Theorem.** Seien  $F$  und  $F'$  zwei unimodulare Fächer. Dann gibt es einen dritten unimodularen Fächer  $F''$  der sowohl aus  $F$  als auch aus  $F'$  durch eine Folge elementarer Verfeinerungen konstruiert werden kann.

Die entsprechende Aussage in allgemeiner Dimension wurde von Tadao Oda 1978 vermutet. Diese „starke Oda-Vermutung“ ist noch immer weit offen. Die „schwache Oda-Vermutung“, dass man in jeder Dimension von jedem unimodularen Fächer zu jedem anderen durch entsprechende Verfeinerungen/Vergrößerungen ist 1997 von Jarosław Włodarczyk bewiesen worden und ist die Grundlage des berühmten schwachen Faktorisierungssatzes von Dan Abramovich, Kalle Karu, Kenji Matsuki und Jarosław Włodarczyk (2002) in der algebraischen Geometrie.

Für den Beweis von Theorem 3.9 brauchen wir drei Lemmata.

**3.10 Lemma.** Sei  $S$  ein Strahl in einem unimodularen Fächer  $F$  erzeugt von  $v$  und seien  $K = \text{cone}(w, v)$  und  $K' = \text{cone}(v, w')$  die beiden Kegel in  $F$ , die  $S$  enthalten.

- (1) Dann ist  $v$  genau dann eine Ecke von  $\text{conv}(0, w, v, w')$  wenn  $f_F(S) \leq 1$
- (2) Aber die Vereinigung  $K \cup K'$  ist genau dann ein (spitzer) Kegel wenn  $f_F(S) \geq 1$ .

Beweis.

**3.11 Lemma.** Sei  $K$  ein (spitzer) Kegel. Dann gibt es eine Zerlegung von  $K$  in unimodulare Kegel.

*Beweis.* Betrachte die konvexe Hülle aller Gitterpunkte in  $K$  ausser dem Ursprung  $P := \text{conv}(K \cap \mathbb{Z}^2 \setminus \{0\})$ . Die beschränkten Randsegmente von  $P$  erzeugen Kegel, die  $K$  zerlegen. Jedes solche Segment bildet zusammen mit  $0$  ein Dreieck ohne weitere Gitterpunkte.  $\square$

**3.12 Lemma.** Sei  $F$  ein unimodularer Fächer, der den unimodularen Fächer  $F'$  verfeinert. Dann erhält man  $F$  durch eine Abfolge elementarer Verfeinerungen aus  $F'$ .

*Beweis.* Benutze Induktion über die Anzahl  $r$  der Strahlen in  $F$ , die nicht zu  $F'$  gehören. Wenn  $r = 0$  ist  $F = F'$ .

Wenn  $r \geq 1$  müssen nach Lemma 3.10(2) alle Strahlenparameter  $f_F$  von Strahlen, die nicht zu  $F'$  gehören mindestens 1 sein.

Wenn auf der anderen Seite  $K \in F'$  Strahlen von  $F$  im Inneren enthält, muss die konvexe Hülle aller dieser Strahlenerzeuger mit  $0$  eine Ecke im Inneren von  $K$  haben. Der entsprechende Strahl fällt unter (1) von Lemma 3.10, muss also Parameter  $f_F = 1$  haben.  $\square$

*Beweis (Theorem 3.9).* Die Familie von Kegeln

$$\overline{F} := \{K \cap K' : K \in F, K' \in F'\}$$

ist wieder ein Fächer, der  $F$  und  $F'$  verfeinert. Nach Lemma 3.11 gibt es einen unimodularen Fächer  $F''$ , der  $\overline{F}$  verfeinert.  $\square$

Mit Theorem 3.9 und Übung 3.8 ist unser Hauptresultat, Theorem 3.7, bewiesen. Der Zwölfsatz für reflexive Polygone folgt unmittelbar mithilfe von Lemma 3.6.

**3.13 Korollar.** Die Anzahlen der Randgitterpunkte eines reflexiven Polygons und seines Polaren addieren sich zu zwölf.