Markus P. Brodmann

Brüche und Kurven – Ein Blick auf die Diophantische Geometrie

Skript und Vertiefungstext zu einem Weiterbildungskurs für Lehrerinnen und Lehrer an Maturitätsschulen

Institut für Erziegungswissenschaften / Institut für Mathematik
Universität Zürich

Einleitung

Der vorliegende Skript ist konzipiert als Begleit- und Vertiefungstext zu einem Weiterbildungsnachmittag zum Thema „Brüche und Kurven – ein Blick auf die Diophantische Geometrie“ für Lehrinnen und Lehrer an Maturitätsschulen. Kurs und Text folgen dem Leitgedanken der *fachwissenschaftlichen Vertiefung mit pädagogischer Ausrichtung*. Der Text enthält – im Sinne der “fachwissenschaftlichen Vertiefung” – ganz wesentlich mehr Material, als im Rahmen eines Nachmittags behandelt werden kann. Dadurch soll den Kursteilnehmerinnen und Kursteilnehmern die Möglichkeit geboten werden, den im Kurs besprochenen Stoff aus eigener Initiative zu vertiefen, was durchaus auch selektiv geschehen darf. Aus diesem Grund haben wir versucht, den Text so zu gestalten, dass er auch zum Selbststudium benutzt werden kann. Wir werden an Schluss dieser Einleitung auch einige *Tipps zum Selbststudium* geben.

Unser Kurs und der vorliegende Begleittext sollen in erster Linie *vertieftes Hintergrundwissen* für den Unterricht an Maturitätsschulen vermitteln. Entsprechend gehen wir beim behandelten Stoff wenig über das hinaus, was im Bereich der Arithmetik schon an der Sekundar- und Mittelschule zur Sprache kommt. Dies entspricht dem Aspekt der ”pädagogischen Vertiefung“. Dafür soll mit grösserer Strenge und Systematik vorgegangen werden, als dies in der Schule möglich ist. Dies geschieht natürlich wieder vor dem Hintergrund der “fachwissenschaftlichen Vertiefung“.
Bei der Auswahl der im Einzelnen behandelten Themen liessen wir uns aber auch vom Aspekt der ”pädagogischen Vertiefung“ leiten. Denn vieles was im Kurs – aber auch im Begleittext – zur Darstellung kommt, lässt sich unseres Erachtens direkt ins Klassenzimmer übertragen. Es geht allerdings um Dinge, die nicht zum Standard-Stoff des Lehrplans gehören. Denn die Behandlung von Schulstoff im Engeren Sinne ghört ja primär in die direkte didaktische Weiterbildung. Wir hoffen aber, dass das eine oder andere Thema doch auch im Schulunterricht seinen Niederschlag findet. In diesem Sinne geben wir in unserer Einleitung auch einige Hinweise zur Frage *”Was ist geeignet für das Klassenzimmer“*.

Behandelt werden folgende vier Themen, denen je ein eigenes Kapitel gewidmet ist:

- Diophantische Gleichungen
- Homogene quadratische Gleichungen

- Rationale Punkte auf Quadriken
- Rationale Punkte auf Kurven höheren Grades: Ein Ausblick

Im ersten Kapitel behandeln wir einige Typen diophantischer Gleichungen, ohne Anspruch auf Systematik und Vollständigkeit zu erheben. Zunächst geht es uns um *lineare diophantische Gleichungen in zwei Unbekannten*. Von diesen speziellen Gleichungen gelangen wir dann zu den diophantischen Gleichungen der Form $ax + by = f(z)$, wo a und b ganze Zahlen und $f(z)$ ein ganzzahliges Polynom in z ist. In diesen einfachen Fällen lässt sich in unserem Rahmen eine systematische Behandlung realisieren. Danach befassen wir uns mit den diophantischen Gleichungen $x^n + y^n = z^n$ ($n \in \mathbb{Z}_{\geq 2}$), wobei wir naturgemäss die Fälle $n = 2$ und $n > 2$ getrennt besprechen... Im Sinne der interdisziplinären Zielsetzung dieses Kurses wollen wir das Lösen dieser diophantischen Gleichungen auch geometrisch als die Suche nach Gitterpunkten auf einer Fläche verstehen.
Im Fall der Gleichungen $x^n + y^n = z^n$ werden wir einen Gedanken vorwegnehmen, welcher später die Motivation für das zweite Kapitel liefert: den Zusammenhang zwischen den Lösungen einer solchen Gleichung – also den Gitterpunkten auf dem durch die Gleichung definierten Kegel – und den rationalen Punkten auf einem horizontalen Schnitt durch diesen Kegel. Als horizontale Schnitte werden wir so die *Fermatkurven* finden und bereits die Frage nach rationalen Punkten auf einer Kurve als zahlentheoretisch relevant erkennen können.
Schliesslich streifen wir – im Sinne einer Schnupperlehre und nicht einer systematischen Behandlung – die *Gleichungen vom Pell'schen Typ*. Eine systematische Behandlung dieses Themas müsste sinnvollerweise die Kettenbruchentwicklung einbeziehen. Doch die Kettenbrüche ihrerseits ordnen sich dem Thema „Zahlen darstellen“ unter, das sich in diesem Kurs nicht mehr einbringen liess...

Kapitel 2 behandelt eine Klasse diophantischer Gleichungen, an der sich der Dualismus zwischen Arithmetik und Geometrie gut demonstrieren lässt: die *homogenen quadratischen diophantischen Gleichungen*. Um die Thematik einzuführen, werfen wir zuerst einen Blick auf die *pythagoräischen Tripel*, welche wir unter Zuhilfenahme einer rationalen Parametrisierung des Kreises bestimmen. Der Rückgriff auf eine solche Parametrisierung wäre an sich nicht notwendig; wir nehmen ihn aber vor, um an einem expliziten Beispiel nochmals die arithmetische Relevanz der Frage nach den rationalen Punkten auf einer Kurve vor Augen zu führen. Dann wenden wir uns den allgemeinen homogenen quadratischen diophantischen Gleichungen zu. Auch für diese diskutieren wir kurz den Zusammenhang zwischen den Lösungen und Punkten auf einer geeigneten ebenen Kurve. Im Anschluss daran befassen wir uns kurz mit der Frage, wann eine rationale Quadrik überhaupt rationale Punkte besitzt. Das sogenannte *Hasseprinzip*, das diese Frage allgemein beantwortet, übersteigt allerdings den Rahmen dieses Kurses. Wir werden uns also mit der Behandlung von Einzelfällen begnügen.

Was uns im Falle des Einheitskreises gelungen ist – nämlich die Parametrisierung aller rationalen Punkte – soll in Kapitel 3 auf beliebige (nichtausgeartete) *Quadriken* übertragen werden. Wir befassen uns dazu als erstes eingehend mit den ebenen Quadriken und deren Verhalten beim Schneiden mit Geraden. Im Sinne eines „Vertiefungsangebots“ sind wir hier bewusst ausführlicher als dies in der zur Verfügung stehenden Kurszeit möglich ist. Wir hoffen aber, dass mindestens einige Kursteilnehmende dies als Einladung verstehen, sich etwas eingehender mit der ebenen „analytischen“ (genauer algebraischen) Geometrie zu befassen.
Nach diesen allgemeinen Vorbereitungen werden wir dann Quadriken rational parametrisieren und so die in Kapitel 3 für den Einheitskreis angewandte Parametrisierungsmethode verallgemeinern. Insesondere werden wir mit dieser Methode aus einem einzigen rationalen Punkt auf einer rationalen Quadrik alle rationalen Punkte dieser Quadrik bestimmen können.

In Kapitel 4 geben wir schliesslich einen Ausblick auf die homogenen diophantischen Gleichungen vom Grad $n > 2$ in drei Unbekannten. Auch hier werden wir die Suche nach den ganzzahligen Lösungen einer solchen Gleichung auf das Aufsuchen rationaler Punkte auf geeigneten ebenen Kurven zurückführen. Das Schwergewicht in diesem Kapitel legen wir auf den Fall $n = 3$, der uns auf die *elliptischen Kurven* führt, ein zentrales Thema von aussergewöhnlicher Reichhaltigkeit, das auch heute noch mit zahlreichen ungelösten Problemen aufwartet. Wir werden insbesondere die *Gruppenstruktur* der elliptischen Kurven einführen (dabei allerdings den Nachweis der Assoziativität nicht erbringen) und den *Satz von Mordell* formulieren, der besagt, dass die rationalen Punkte einer elliptischen Kurve eine endlich erzeugte abelsche Gruppe bilden.
Schliesslich weisen wir auch auf den faszinierenden Zusammenhang hin, der zwischen der Theorie der elliptischen Kurven und dem von *Taylor und Wiles geführten Beweis der Fermat-Vermutung* besteht. Dazu führen wir die *Frei'sche elliptische Kurve* zu einem Tripel $(p, x, y) \in \mathbb{N}(p$ eine Primzahl > 2 ein. Wir führen (in sträflich knapper Weise) den Begriff der Modulfunktion ein, um die *Modularitäsvermutung von Taniyama-Shimura* formulieren zu können. Damit können wir auch den ıNicht-Modularitätssazt von Ribet für die Frey'schen elliptischen Kurven formulieren. Den für die Formulierung des *Modularitätssatzes von Taylor-Wiles* benötigten Begriff der *semistabilen elliptischen Kurve* werden wir allerdings nicht mehr einführen.
Ganz kurz weisen wir auch auf die überraschende Anwendung hin, welche die – über endlichen Körpern definierten – elliptischen Kurven im Bereich der Kryptographie gefunden haben. Hier wird uns ein Beispiel vor Augen geführt, wie ein Gebiet, das lange Zeit als völlig "anwendungsfern“ beurteilt wurde, sozusagen "über Nacht“ von grösster Bedeutung für gewisse Anwendungen werden kann.
Ganz zum Schluss weisen wir noch auf den Fall hin, in welchem der Grad n unserer homogenen diophantischen Gleichung > 3 ist und formulieren den *Satz von Faltings*, d.h. die durch Faltings bewiesene *Mordell-Vermutung*.

WAS IST GEEIGNET FÜR DAS KLASSENZIMMER ?

- *Kapitel 1:* Lineare Diophantische Gleichungen in zwei unbekannten sind ein Thema, das sicher in der Schule behandelt werden kann, und oft auch wird. Voraussetzung ist lediglich, dass die Klasse schon mit linearen Gleichungen in zwei Unbekannten vertraut ist. Empfehlenswert wird es sicher sein, mit einem Beispiel zu beginnen, wie etwa das in Aufgabe 1.4 A) vorgeschlagene. Das Grundverständnis, dass es hier darum geht, auf einer gegeben Gerade *ganzzahlige Gitterpunkte* zu suchen, kann wohl mit Hilfe eines Beispiels am besten geweckt werden. Natürlich sollte man noch weitere Beispiele folgen lassen, etwa solche, bei welchen die linearen Koeffizienten nicht teilerfremd sind. Dann knnte man auch das in Bemerkung 1.3 B) gegebene Lsungsrezept angeben und erklären. Auch könnte man in einem Beispiel den minimalen Abstand zweier verschiedener Lösungen mit Hilfe des Satzes von Pythagoras berechnen.
  Auch der Fall von diophantischen Gleichungen der Form $ax + by = f(z)$ lsst sich fr einfache Funktionen $f(z)$ durchaus in der Schule behandeln. Zur Einfhrung des Themas knnten die in den Aufgaben 1.6 A),B),C) betrachteten Beispiele durchaus geeignet sein. Das in den Bemerkungen 1.5 A),B) Gesagte ist natrlich für das tiefere Verständnis unerlässlich, kann aber an Hand der vorgeschlagenen Einführungsbeispiele sicher konkret erarbeitet werden. Das Grundverständnis, dass es hier darum geht, ganzahlige Gitterpunkte auf einer gegebenen Fläche im Raum zu suchen, sollte anhand dieser Beispiele einleuchtend vermittelt werden können.
  Auch die Ausführungen zu den Gleichungen vom Typ $x^n + y^n = z^n$ gemäss Beispiel 1.7 übersteigen nicht das, was an der Schule behandelt werden kann. Die Historische Bedeutung dieser Gleichungen wre es Wert, dem Thema vielleicht einmal wenn mglich eine Lektion zu widmen. Auch hier geht es um die Suche nach Gitterpunkten auf einer Fläche, dass sich aber auf die Suche von rationalen Punkten auf den durch $u^n + v^n = 1$ definierten ebenen Kurven reduzieren lässt, den *Fermatkurven*.

- *Kapitel 2:* Geeignet für eine mögliche Behandlung in der Schule sind hier natürlich mit Sicherheit die Kernthemen des ganzen Kapitels: die *pythagoräische Tripel* und deren geometrische Gewinnung aus den rationalen Punkten auf dem Einheiskreis. So können wohl die in Defintion und Bemerkung 2.1 eingefürten *pythagoräische Tripel* in gleicher Weise im Schulunterricht definiert und erklärt werden. Natürlich sollte dann mindestens ein Teil der Aufgaben 2.2 auch diskutiert werden, damit das Thema konkret wird und "Spass macht".
  Die *(rationale) Parametrisierung des Einheitskreises* gemäss Konstruktion (2.3) lässt sich mit Sicherheit schon in der Schule behandeln. Die zuhörigen Aufgaben 2.4 sind zur Vertiefung des Stoffes im Unterricht wohl ebenfalls gut geeignet.

Schliesslich kann auch das Ziel dieser Bemühungen – das Aufsuchen von pythagoräischen Tripeln (s. Bemerkung und Definition 2.5, Satz 2.6, Aufgaben 2.7) ohne Probleme und wohl auch mit Gewinn zum Unterrichtsthema gemacht werden. Die Beispiele 2.15 und 2.16, aber auch die Aufgabe 2.17 A) können in der Schule behandelt werden und wecken hoffentlich bei einigen der Schülerinnen und Schülern ein vertieftes Interesse an etwas "unkonventionellen" mathematischen Aktivitäten.

- *Kapitel 3:* Dieses Kapitel benötigt zwar in der Tat nicht mehr mathematische Vorkenntnisse als die Mittelschule vermittelt, ist asber trotzdem primär für ein allfälliges Selbsstudium durch die Lehrerinne und Lehrer konzipiert. Es ist aber von der Fülle des Stoffes und der strengen Vorgehensweise kaum mehr für die ¨bertragung in den Schulunterricht geeignet. Als einzigen Unterrichts-relevanter Stoff könnte sich hier das Thema *Kegelschnitte* anbieten, das ja mittlerweile wohl allgemein in den Standardlehrplänen leider kaum mehr etwas zu suchen hat.

- *Kapitel 4:* Auch diese Kapitel richtet sich in erster Linie an Lehrerinnen und Lehrer, welche den präsentierten Stoff im Selbsstudium erarbeiten möchten. Von diesem Hintergrund aus, gibt es aber doch vielleicht die Möglichkeit, das eine ober andere als Anregung für den Unterricht zu verwenden. Warum nicht die Gleichung einer einfachen elliptischen Kurve in affinmer Normalform hinschreiben, die Kurve diskutieren und dann rein geometrisch die Gruppenstruktur (mit dem "unsichtbaren Fernpunkt ∞ als Neutralelement) erklären. Das da im Allgemeinen genau ein *Verbindungspunkt* zu erwarten ist, lässt sich durch parametrisieren der *Verbindungsgeraden* mit dem *Satz von Vieta* leicht direkt verstehen. Warum dann nicht einmal den Mut fassen und darauf hinweisen, dass die Fermat-Vermutung (die ja wirklich schon vielern Schülern ein Begriff ist) mit Hilfe der Theorie "solcher sogenannter elliptischer Kurven" bewiesen wurde. Die Biologen und die Physiker schrecken ja auch nicht davor zurück, im Unterricht Dinge zu behandeln, die genau genommen von den Schülerinnen und Schülern gar nicht verstanden werden können. Noch jetzt ist der Autor seinem damaligen Oberstufen-Mathematiklehrer, Professor Rolf Conzelmann, sehr dankbar, dass er nicht davor zurückschreckte ab und zu einen Ausblick auf Dinge zu geben, die schon jenseits des Schulstoffes lagen. Dies ist wohl eine besonders geeignete Art und Weise, Schlerinnen und Schüler für ein Mathematik-Studium zu motivieren...

TIPPS FÜR DAS SELBSTSTUDIUM

- *Kapitel 1:* Wichtig und grundlegend sind hier die Ausführungen über die linearen diophantischen Gleichungen (1.2–1.4). Zum Verständnis des Stoffes aus Kapitel 2 – und um eine erste Einsicht in den Zusammenhang zwischen Arithmetik und Geometrie zu gewinnen – sollten Sie sich relativ eingehend mit 1.7 und 1.8 befassen, aber auch die zugehörigen Aufgaben 1.9 mindestens zum Teil lösen. Das Thema

der Pell'schen Gleichungen wird nicht umfassend behandelt, sondern eher als eine Einladung zum Ausprobieren und Knobeln. Hier sollten Sie (nach einem „Einlesen“ bei 1.10) vor allem den Übungsaufgaben 1.11 Ihre Aufmerksamkeit schenken.

- *Kapitel 2:* Als Weg durch dieses Kapitel bietet sich etwa an: 2.1, mindestens ein Teil der Aufgabe 2.2, die rationale Parametrisierung des Einheitskreises (2.3) und die Bestimmung der pythagoräischen Tripel mit Hilfe des Satzes von Diophantos (2.6). Einige der Aufgaben aus 2.7 zu lösen wird ebenfalls empfohlen. Nicht schaden kann es auch, nochmals die in 2.8 rekapitulierte Idee durchzugehen. Zum Thema der homogenen quadratischen diophantischen Gleichungen im allgemeinen (2.11) empfehlen wir vor allem auch die Aufgaben 2.12 und 2.14. Dem Beispiel 2.15 und den Aufgaben 2.17 sollen Sie ebenfalls Bedeutung beimessen.

- *Kapitel 2:* Dieses Kapitel ist zum grossen Teil auf direkte Umsetzung in den Schulunterricht angelegt. Trotzdem ist es auch zum Selbststudium geeignet. Als Weg für das Selbststudium durch dieses Kapitel bietet sich etwa an: 2.1, mindestens ein Teil der Aufgabe 2.2, die rationale Parametrisierung des Einheitskreises (2.3) und die Bestimmung der pythagoräischen Tripel mit Hilfe des Satzes von Diophantos (2.6). Einige der Aufgaben aus 2.7 zu lösen wird ebenfalls empfohlen. Nicht schaden kann es auch, nochmals die in 2.8 rekapitulierte Idee durchzugehen. Zum Thema der homogenen quadratischen diophantischen Gleichungen im allgemeinen (2.11) empfehlen wir vor allem auch die Aufgaben 2.12 und 2.14. Dem Beispiel 2.15 und den Aufgaben 2.17 sollen Sie ebenfalls Bedeutung beimessen.

- *Kapitel 3:* Lassen Sie sich vom Umfang dieses stark auf „freiwillige Vertiefung“ ausgerichteten Kapitels nicht entmutigen. Auch „Eilige“ sollten die Vorbetrachtung in 3.1–3.3 mindestens intensiv durchlesen und die zugehörigen Aufgaben 3.4 nicht ganz verschmähen. Was hier zur Sprache gebracht wird ist „klassische mathematische Kultur“. Wer mehr Zeit investieren kann und sich von etwas anspruchsvolleren Gedankengängen nicht abschrecken lässt, ist eingeladen weiter vorzudringen – etwa bis zum Hauptsatz 3.24. Der Weg bis zu diesem Meilenstein ist sicher nicht mit lockerem Schlendern zu schaffen – aber er ist so angelegt, dass er sich mit den Kenntnissen der Mittelschulmathematik, einem klaren Kopf und etwas Hartnäckigkeit begehen lässt. Wer „blindlings“ der Algebra vertraut und auf die geometrische Anschauung verzichten will kann auf diesem Weg auch 3.6, 3.16, 3.17, 3.18 D) und 3.19 überspringen. Wenn Sie bis zum Etappenziel 3.24 gelangt sind, haben Sie sich vermutlich genügend „Fitness“ erworben, um auch den verbleibenden kleinen Rest des Kapitels mit Leichtigkeit zu bezwingen...

- *Kapitel 4:* Hier gilt im Grundsatz das Gleiche wie für das vorangehende Kapitel: Lassen Sie sich nicht abschrecken, sondern wagen Sie vielleicht einen Versuch,

das eine oder andere in diesem Kapitel zu vestehen. Der am Anfang des Kapitels gegebene Überblick motiviert Sie vielleicht dazu, den Einstieg zu wagen. Damit Sie etwas genauer wissen, worum es in diesem Kapitel überhaupt geht, sollten Sie vielleicht zuerst die Definitionen 4.1, Bemerkung und Definition 4.2 lesen und einige der Aufgaben 4.3 lösen. Empfehlenswert ist s dann, die beiden vorbereitenden Abschnitte "Univariate Polynome" und "Bivariate Polynome" durchzugehen, und dabei möglichst viele der gestellten Aufgaben zu lösen. Auch das Thema "Kritische Geraden und Tangenten" ist für das Spätere bedeutsam. Den Satz 4.18 und das in den Aufgaben für den Beweis Bereitgestellte ist die unvezichtbare Quintessenz dieses Themas. Mit dem Thema "Fernpunkte" werfen Sie einen empfehlenswerten Blick in die projektive Geometrie, den man hier im Hinblick auf die Abbildung 4.1 auch wörtlich verstehen kann.
Das Thema "elliptische Kurven" sei Ihnren Aufmerksamkeit ganz besonders empfohlen. Den Abschnitt "elliptische Kurven und die Fermat-Vermutung" können Sie ruhig wie einen Wissenschaftsbeitrag in der Wochendbeilage einer Tageszeitung lesen, also mit einem zeitgenössischen "Touch von Infotainment". Das Gleiche gilt für den verbleibenden Kurzabschnitt "Diophantische Formen vom Grad > 3".

Bezeichnungen. Mit $\mathbb{Z}$ werde der Ring der ganzen Zahlen bezeichnet. Ist $n \in \mathbb{Z}$, so schreiben wir

$$\mathbb{Z}_{\geq n} := \{m \in \mathbb{Z} \mid m \geq n\}.$$

Wir verwenden auch die Bezeichnungen

$$\mathbb{N}_0 := \mathbb{Z}_{\geq 0} \text{ und } \mathbb{N} := \mathbb{Z}_{\geq 1}.$$

Mit $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ sei respektive der Körper der rationalen, der reellen und der komplexen Zahlen bezeichnet.

Kapitel 1

Diophantische Gleichungen

Überblick

Diophantische Gleichungen sind (algebraische) Gleichungen mit ganzzahligen Koeffizienten in zwei oder mehr Unbekannten, bei welchen man nur nach den ganzzahligen Lösungen fragt. Diese Gleichungen werden so benannt nach Diophantos von Alexandria (3. Jh.).

Beispiele von diophantischen Gleichungen sind etwa

(1.0) a) $2x - 3y = 5$;

b) $x^2 + y^2 = z^2$;

c) $x^n + y^n = z^n$ $(n = 3, 4, \ldots)$;

d) $x^2 - 7y^2 = 1$;

d') $x^2 - 410286423278424y^2 = 1$.

Die Gleichung a) ist eine sogenannte *lineare diophantische Gleichung*. Vielleicht haben Sie diese Art Gleichung schon in der Schule kennen und lösen gelernt. Es handelt sich um Gleichungen, die schon in der früheren Antike und im alten China ausgiebig studiert wurden.

Die unter b) genannte diophantische Gleichung werden wir im nächsten Kapitel noch eingehender diskutieren. Die in c) aufgeführten diophantischen Gleichungen sind vielleicht die „berühmtesten“ diophantischen Gleichungen überhaupt. Auch auf diese Gleichungen werden wir in diesem Kapitel nochmals zurückkommen.

Die unter d) und d') genannten diophantischen Gleichungen sind sogenannte *Pell'sche Gleichungen*. Dieser Typ von Gleichungen wurde schon in der griechischen Antike, aber

auch von den indischen und arabischen Mathematikern des 7. bis 12. Jahrhunderts studiert und hat bis heute immer wieder das Interesse von Forschern und Tüftlern gefunden.

Mit diesem kleinen „Bouquet berühmter Gleichungen“ soll angetönt werden, dass wir uns mit den diophantischen Gleichungen in einem Kerngebiet der Zahlentheorie bewegen.

Zunächst ist das Lösen solcher diophantischer Gleichungen ein rein arithmetisches Problem. Doch ist es ein wichtiges Anliegen dieses Kapitels, auch die geometrische Natur dieses arithmetischen Problems aufzuzeigen. Mindestens andeutungsweise wagen wir damit den Blick in eine Richtung zu wenden, die sich in den letzten Jahrzehnten als besonders fruchtbar für die Zahlentheorie erwiesen hat: die *diophantische Geometrie*. Allerdings werden wir auch hier auf dem Boden der elementaren Arithmetik bleiben müssen, denn für Höhenflüge reicht unser „mathematischer Treibstoff“ nicht aus.

Folgende Themen werden wir in diesem Kapitel behandeln:

- *Lineare diophantische Gleichungen mit zwei Unbekannten,*
- *Gleichungen der Form* $ax + by = f(z)$,
- *Die Gleichungen* $x^n + y^n = z^n$,
- *Pell'sche Gleichungen.*

Vom Stil her gesehen handelt es sich bei diesem Kapitel um eine „Schnupperlehre in Diophantik“ : Wir werden, ausser bei der Behandlung der linearen diophantischen Gleichungen, keine allgemeinen Sätze beweisen. Vielmehr wollen wir Einzelfälle und Beispiele betrachten, um so an das Gebiet der diophantischen Gleichungen heranzuführen.

Lineare diophantische Gleichungen mit zwei Unbekannten

Zuerst befassen wir uns mit diophantischen Gleichungen des in 1.0 a) genannten Typs, d.h. mit diophantischen Gleichungen der Form

$$ax + by = c \ (a, b, c \in \mathbb{Z}).$$

Dabei interessieren wir uns für *ganzzahlige Lösungen* dieser Gleichung, also für Lösungspaare $(x, y) \in \mathbb{Z}^2$. Wir werden ein Kriterium dafür angeben, dass die lineare diophantische Gleichung $ax + by = c$ überhaupt ganzzahlige Lösungen hat und eine Methode entwickeln, um diese Lösungen zu finden.

Wir beginnen mit dem folgenden Hilfsresultat.

Lemma 1.1. *Seien* $a, b \in \mathbb{Z}\backslash\{0\}$. *Seien* $w, z \in \mathbb{Z}$ *mit* $aw + bz = 0$. *Dann gibt es ein* $t \in \mathbb{Z}$ *so, dass* $w = \frac{tb}{\mathrm{ggT}(a,b)}$ *und* $z = \frac{-ta}{\mathrm{ggT}(a,b)}$.

Beweis: Sei $g = \mathrm{ggT}(a,b)$. Dann sind $\frac{a}{g}$ und $\frac{b}{g} \in \mathbb{Z}$ und es gilt $\frac{a}{g}w + \frac{b}{g}z = 0$, also

$$(\alpha) \qquad \frac{a}{g}w = -\frac{b}{g}z.$$

Nach 4.16 b) gibt es Zahlen $s, r \in \mathbb{Z}$ mit $as + br = g$. Es folgt $\frac{a}{g}s + \frac{b}{g}r = 1$, also mit Hilfe von (α)

$$\begin{aligned} w = 1 \cdot w &= \left(\frac{a}{g}s + \frac{b}{g}r\right) w = \\ &= s\frac{a}{g}w + rw\frac{b}{g} = -s\frac{b}{g}z + rw\frac{b}{g} = \\ &= (-sz + rw)\frac{b}{g}. \end{aligned}$$

Mit $t := -sz + rw$ folgt also $w = t\frac{b}{g}$. Mit (α) folgt $-\frac{b}{g}z = \frac{a}{g}w = \frac{b}{g}\frac{a}{g}t$, d.h. in der Tat auch $z = -\frac{a}{g}t$. ■

Im folgenden Satz werden die linearen diophantischen Gleichungen abschliessend behandelt.

Satz 1.2. *Seien $a, b \in \mathbb{Z}\backslash\{0\}$ und $c \in \mathbb{Z}$. Dann gelten:*

a) *Die Gleichung*

$$ax + by = c$$

besitzt genau dann eine ganzzahlige Lösung $(x_0, y_0) \in \mathbb{Z}^2$, wenn $\mathrm{ggT}(a,b)|c$.

b) *Ist $(x_0, y_0) \in \mathbb{Z}^2$ eine Lösung der obigen Gleichung und ist $(x, y) \in \mathbb{Z}^2$ ein weiteres Paar ganzer Zahlen, so gilt*

$$ax + by = c$$

genau dann, wenn es eine Zahl $t \in \mathbb{Z}$ gibt mit

$$x = x_0 + t\frac{b}{\mathrm{ggT}(a,b)} \text{ und } y = y_0 - t\frac{a}{\mathrm{ggT}(a,b)}.$$

Beweis: Sei $g := \mathrm{ggT}(a,b)$. „a)“ : Nehmen wir zunächst an, unsere Gleichung habe eine ganzzahlige Lösung $(x_0, y_0) \in \mathbb{Z}^2$, sodass $ax_0 + by_0 = c$. Wegen $g|a$ und $g|b$ folgt dann $g|c$.

Es gelte umgekehrt $g|c$. Mit einer geeigneten Zahl $d \in \mathbb{Z}$ gilt dann $c = dg$. Nach 4.16 b) gibt es Zahlen $u, v \in \mathbb{Z}$ mit $au + bv = g$. Mit $x_0 := ud$ und $y_0 := vd$ folgt dann $ax_0 + by_0 = c$. Also ist (x_0, y_0) eine ganzzahlige Lösung unserer Gleichung.

„b)“ : Sei $t \in \mathbb{Z}$ und seien $x = x_0 + t\frac{b}{g}$ und $y = y_0 - t\frac{a}{g}$. Dann folgt $ax + by = a(x_0 + t\frac{b}{g}) + b(y_0 - t\frac{a}{g}) = ax_0 + by_0 + t(a\frac{b}{g} - b\frac{a}{g}) = ax_0 + by_0 + t \cdot 0 = c$.

Sei umgekehrt $(x, y) \in \mathbb{Z}^2$ mit $ax + by = c$. Es folgt $a(x - x_0) + b(y - y_0) = ax + by - ax_0 - by_0 = c - c = 0$, also $\frac{a}{g}(x - x_0) + \frac{b}{g}(y - y_0) = 0$. Nach 1.1 gibt es ein $t \in \mathbb{Z}$ mit $x - x_0 = \frac{b}{g}t$ und $y - y_0 = -\frac{a}{g}t$. Es folgen $x = x_0 + \frac{b}{g}t$ und $y = y_0 - \frac{a}{g}t$. ■

Bemerkungen 1.3. A) Leicht prüft man nach, dass die Aussagen a) und b) im Satz 1.2 auch richtig sind, wenn eine der beiden Zahlen a oder b Null ist.

B) Satz 1.2 und sein Beweis belehren uns darüber, wie wir die Lösungsmenge

a) $$\mathbb{L} := \{(x, y) \in \mathbb{Z}^2 | ax + by = c\}$$

der diophantischen Gleichung $ax + by = c$ (mit $(a, b) \neq (0, 0)$) bestimmen:

Sei $g := \mathrm{ggT}(a, b)$ und seien $u, v \in \mathbb{Z}$ mit $au + bv = g$. Ist $g \nmid c$, so ist $\mathbb{L} = \emptyset$. Sei also $g|c$. Dann sieht man aus dem Beweis von 1.2, dass das Zahlenpaar

$$(x_0, y_0) := \left(\frac{c}{g}u, \frac{c}{g}v\right)$$

eine Lösung unserer diophantischen Gleichung ist. Nach 1.2 b) folgt deshalb

b) $$\mathbb{L} = \left\{ \left(\frac{c}{g}u + t\frac{b}{g}, \frac{c}{g}v - t\frac{a}{g} \right) \middle| \, t \in \mathbb{Z} \right\}.$$

C) Geometrisch können wir das Lösen unserer diophantischen Gleichung leicht verstehen:

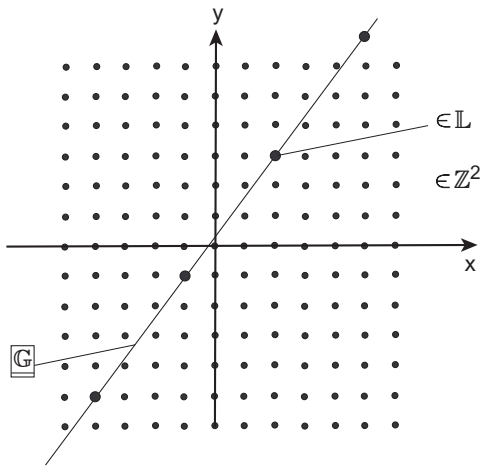


Abbildung 1.1: Lösungen der diophantischen Gleichung $4x - 3y = -1$

Die *reelle Lösungsmenge*

$$\mathbb{G} := \{(x, y) \in \mathbb{R}^2 | ax + by = c\}$$

entspricht einer *Geraden* in der Ebene $\mathbb{R}^2$. Die ganzzahlige Lösungsmenge $\mathbb{L}$ ist die Menge $\mathbb{G} \cap \mathbb{Z}^2$ der *Gitterpunkte* auf der Geraden $\mathbb{G}$, d.h. der Geradenpunkte mit ganzzahligen Koordinaten. •

Aufgaben 1.4. A) Lösen Sie die diophantische Gleichung $-x + 2y = 3$ und skizzieren Sie die Situation.

B) Geben Sie alle möglichen diophantischen Gleichungen $ax + by = c$ an, welche im Rechteck $\{(x, y) | 0 \leq x \leq 2, 0 \leq y \leq 1\}$ mindestens 2 verschiedene Lösungen haben.

C) Geben Sie alle möglichen diophantischen Gleichungen $ax + by = 1$ an, welche zwei verschiedene Lösungen mit einem Abstand echt kleiner als 4 besitzen (nur Fälle mit $ab \neq 0$).

D) Seien $a, b, c \in \mathbb{Z}$ mit $a, b \neq 0$ und $\mathrm{ggT}(a, b) | c$. Geben Sie den kleinstmöglichen Abstand d zweier verschiedener Lösungen der diophantischen Gleichung $ax + by = c$ in der Ebene $\mathbb{R}^2$ an.

E) Seien $a, b, c \in \mathbb{Z}$ und $d \in \mathbb{R}$ definiert wie in Aufgabe D). Sei $\delta := \frac{c}{\sqrt{a^2+b^2}}$. Zeigen Sie:

a) Der Nullpunkt hat von der durch $ax + by = c$ definierten Geraden den Abstand $|\delta|$.

b) Die diophantische Gleichung $ax + by = c$ hat mindestens eine und höchstens zwei ganzzahlige Lösungen $(x, y) \in \mathbb{Z}^2$ mit einem Abstand kleiner oder gleich $\sqrt{\delta^2 + \frac{d^2}{4}}$ vom Nullpunkt.

F) Bestimmen Sie alle ganzzahligen Lösungen $(x, y) \in \mathbb{Z}^2$ der Gleichung $2x^2 - 3y^2 - 5xy + x + 11y = 6$. (*Hinweis:* Zerlegung in Linearfaktoren.) •

Gleichungen der Form $ax + by = f(z)$

Gewisse einfache diophantische Gleichungen mit drei Unbekannten lassen sich mit dem in 1.3 beschriebenen Verfahren ebenfalls lösen. Wir führen dazu die nachfolgenden Gedanken an:

Bemerkungen 1.5. A) Sei $f(z)$ ein ganzzahliges Polynom. Seien $a, b \in \mathbb{Z}\backslash\{0\}$. Wir möchten die diophantische Gleichung

a) $$ax + by = f(z)$$

lösen, d.h. alle ganzzahligen Lösungstripel $(x, y, z) \in \mathbb{Z}^3$ der Gleichung a) finden. Dazu kann man wie folgt vorgehen:

Zuerst sucht man wieder zwei Zahlen $u, v \in \mathbb{Z}$ mit $au + bv = \mathrm{ggT}(a, b) =: g$. Nach 1.3 B) ist dann klar, dass die Lösungen der diophantischen Gleichung a) gerade die Zahlentripel der Form

b) $$\left(\frac{f(z)}{g}u + t \cdot \frac{b}{g}, \frac{f(z)}{g}v - t\frac{a}{g}, z\right);\ (t, z \in \mathbb{Z}, g|f(z))$$

sind. Für beliebiges f ist die Bedingung $g|f(z)$ nicht leicht zu kontrollieren. Deshalb führt diese Methode eigentlich nur im Fall wo a und b teilerfremd sind, d.h. wo $g = 1$ gilt, sicher zu Ziel.

B) Geometrisch kann man die soeben gelöste Aufgabe so verstehen: Die Menge aller reellen Lösungen (x, y, z) der Gleichung a) bildet eine Fläche $\mathbb{F}$ im Raum $\mathbb{R}^3$. Die ganzzahligen Lösungen b) sind die Gitterpunkte dieser Fläche, d.h. die Punkte der Menge $\mathbb{F} \cap \mathbb{Z}^3$.

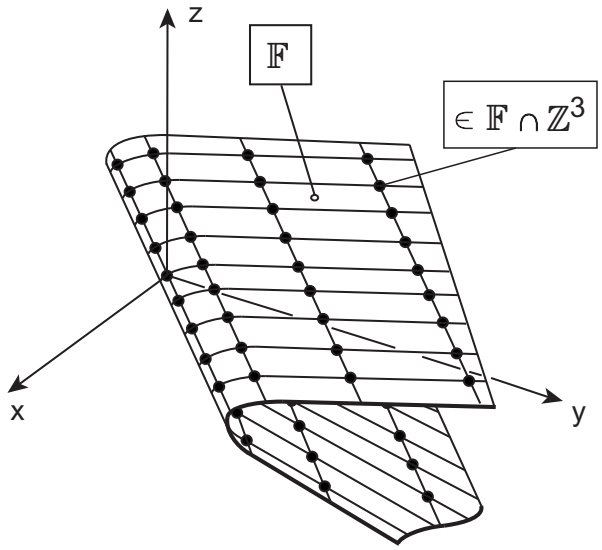


Abbildung 1.2: Lösungen von $ax + by = f(z)$

•

Aufgaben 1.6. A) Lösen Sie die diophantische Gleichung

$$x + y = z$$

gemäss 1.5 und skizzieren Sie den geometrischen Sachverhalt.

B) Lösen Sie Aufgabe A) mit der diophantischen Gleichung

$$-x + y = z^2.$$

C) Beschreiben Sie die Menge aller ganzzahligen Lösungstripel (x, y, z) der Gleichung

$$2x - 6y = z^2 + 1.$$

D) Wie muss $b \in \mathbb{Z}$ gewählt werden, damit die diophantische Gleichung

$$5x - by = 10z^4 - 11$$

keine Lösung hat. Welches sind andernfalls ihre Lösungen, falls zudem noch $b \in \{0, 1, 2, 3, 4, 5\}$ gilt? •

Die Gleichungen $x^n + y^n = z^n$

Vielleicht etwas provokativ wollen wir nun die in 1.0 b) und c) genannten Gleichungen zum Anlass einer weiteren Überlegung nehmen. Wir können dabei nämlich wieder etwas Neues über die geometrisch-arithmetische Doppelnatur der diophantischen Gleichungen lernen. Dass die betrachteten Gleichungen für $n \geq 3$ (wie der Leserschaft sicher bekannt ist) keine interessanten ganzzahligen Lösungen haben, stört uns dabei wenig.

Beispiel 1.7. A) Wir wählen $n \in \mathbb{N}$ und betrachten die diophantische Gleichung

a) $$x^n + y^n = z^n.$$

Anders gesagt, wir interessieren uns für die Menge aller Tripel $(x, y, z) \in \mathbb{Z}^3$, welche der obigen Gleichung genügen. Für $n = 1$ sollte uns diese Gleichung keine Schwierigkeiten bieten (s. 1.5). Wir nehmen also an, es sei $n \geq 2$. Natürlich hat die Gleichung a) einfach zu findende Lösungen $(x, y, z) \in \mathbb{Z}^3$, wenn eine der drei Zahlen x, y und z gleich 0 ist. Diese sogenannten *trivialen Lösungen* wollen wir nicht mehr ins Auge fassen. Wir wollen also insbesondere annehmen, es sei $z \neq 0$.

B) Wir missachten alles, was wir im Fall $n \geq 3$ über die Gleichung A) a) schon gelesen und gehört haben und im Fall $n = 2$ vielleicht schon wissen (vgl. 1.6, 1.7, 1.10). Wir fragen also nach Lösungen (x, y, z) der Gleichung A) a) in $\mathbb{Z}^3$ mit $z \neq 0$. Die Ausführungen aus 1.5 legen es nahe, die Anzahl der Unbekannten von 3 auf 2 zu reduzieren. Dies lässt sich in der Tat tun, allerdings auf neuartige Weise:

Ist $(x, y, z) \in \mathbb{Z}^3$ eine Lösung der Gleichung A) a) so, dass $z \neq 0$, dann gilt mit

$$u := \frac{x}{z},\ v := \frac{y}{z} \in \mathbb{Q}$$

die Gleichung

a) $$u^n + v^n = 1.$$

Sind umgekehrt $u, v \in \mathbb{Q}$ mit $u^n + v^n = 1$, so können wir einen gemeinsamen Nenner $z \in \mathbb{Z}\backslash\{0\}$ von u und v suchen. Dann gilt mit

$$x := uz,\ y := vz \in \mathbb{Z}$$

die Beziehung $x^n+y^n = u^n z^n+v^n z^n = (u^n+v^n)z^n = z^n$. Also ist (x, y, z) eine ganzzahlige Lösung der Gleichung A) a). Damit ist gezeigt:

b)
$$\begin{cases} \textit{Sind } u, v \in \mathbb{Q} \textit{ mit } u^n + v^n = 1 \textit{ und ist } z \in \mathbb{Z}\backslash\{0\} \textit{ so, dass} \\ uz, vz \in \mathbb{Z}, \textit{ dann ist das Zahlentripel} \\ \qquad\qquad (uz, vz, z) \in \mathbb{Z}^3 \\ \textit{eine ganzzahlige Lösung der Gleichung } x^n + y^n = z^n. \end{cases}$$

Zudem ist *jede* Lösung der diophantischen Gleichung $x^n + y^n = z^n$ nach dem Verfahren b) zu finden.

Insgesamt kommt es also auf dasselbe heraus, ob wir ganzzahlige Lösungen der Gleichung A) a) oder rationale Lösungen der Gleichung B) a) suchen.

C) Wir wollen uns nun auch Klarheit verschaffen über die Geometrie, die sich hinter dem soeben beschriebenen Konzept verbirgt. Wir betrachten die Menge

a) $$\mathbb{K} := \{(x, y, z) \in \mathbb{R}^3 | x^n + y^n = z^n\}$$

aller *reellen Lösungstripel* $(x, y, z) \in \mathbb{R}^3$ der Gleichung A) a). Dabei fällt uns folgendes auf:

Sind $(x, y, z) \in \mathbb{K}$ und $\lambda \in \mathbb{R}$, so folgt $(\lambda x)^n + (\lambda y)^n = \lambda^n x^n + \lambda^n y^n = \lambda^n(x^n + y^n) = \lambda^n z^n = (\lambda z)^n$, also $(\lambda x)^n + (\lambda y)^n = (\lambda z)^n$, d.h. $(\lambda x, \lambda y, \lambda z) \in \mathbb{K}$. Schreiben wir

$$\mathbb{R}(x, y, z) := \{(\lambda x, \lambda y, \lambda z) | \lambda \in \mathbb{R}\},$$

so gilt also:

b) $$(x, y, z) \in \mathbb{K} \Longrightarrow \mathbb{R}(x, y, z) \subseteq \mathbb{K}.$$

Ist $(x, y, z) \in \mathbb{K}\backslash\{(0, 0, 0)\}$, so ist $\mathbb{R}(x, y, z)$ die durch $(0, 0, 0)$ und (x, y, z) laufende Gerade. Wie wir eben festgestellt haben, liegt diese Gerade ganz in $\mathbb{K}$. Anders gesagt: $\mathbb{K}$ enthält mit jedem Punkt $(x, y, z) \in \mathbb{K}\backslash\{(0, 0, 0)\}$ auch die ganze Gerade durch $(0, 0, 0)$ und den Punkt (x, y, z). Damit ist $\mathbb{K}$ ein sogenannter *Kegel mit Spitze* $(0, 0, 0)$.

Wir halten die Situation in der nachfolgenden Skizze fest, für welche wir $n = 2$ gewählt haben.

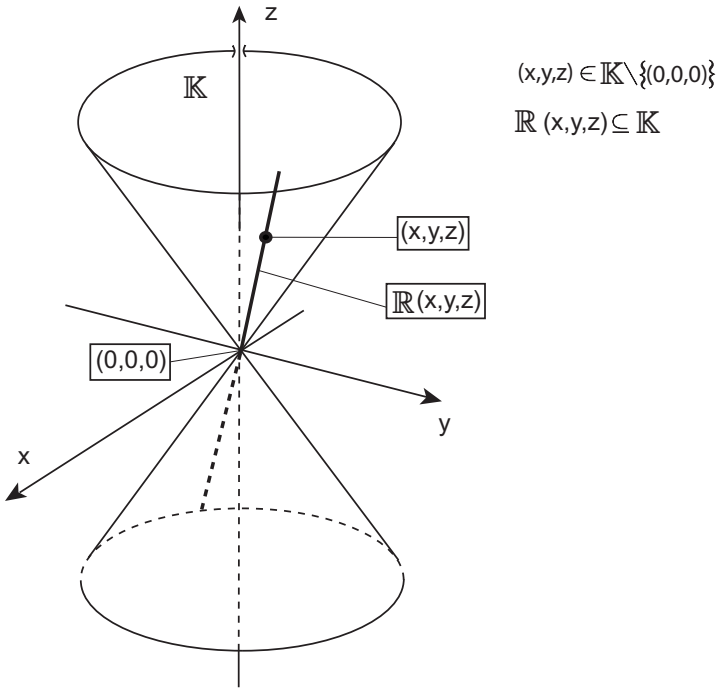


Abbildung 1.3: Kegel zur Gleichung $x^2 + y^2 = z^2$

D) Wir sind allerdings nicht an allen reellen Lösungstripeln der Gleichung A) a) interessiert, sondern nur an der Menge

$$\mathbb{K} \cap \mathbb{Z}^3 = \{(x, y, z) \in \mathbb{Z}^3 | x^n + y^n = z^n\}$$

der ganzzahligen Lösungstripel der Gleichung A) a). Anders gesagt: Uns interessieren *Gitterpunkte auf* $\mathbb{K}$. In B) b) haben wir bereits angegeben, wie man diese Gitterpunkte erhält, wenn man die rationalen Lösungspaare $(u, v) \in \mathbb{Q}^2$ der Gleichung B) a) kennt. Die Gleichung B) a) erhält man aber aus der Gleichung A) a), indem man $z = 1$ setzt und u resp. v für x resp. y schreibt. Das Lösen der Gleichung B) a) entspricht also dem

Schneiden des Kegels $\mathbb{K}$ mit der durch $z = 1$ definierten Ebene $\mathbb{E}$. Das Aufsuchen der rationalen Lösungen von B) a) entspricht deshalb dem Aufsuchen aller Punkte $(u, v, 1)$ auf der Schnittkurve $\mathcal{C} := \mathbb{E} \cap \mathbb{K}$ mit $(u, v) \in \mathbb{Q}^2$. Hat man einen solchen Punkt $(u, v, 1)$ gefunden, so sucht man einen gemeinsamen Nenner z von u und v und erhält so den Gitterpunkt $(uz, vz, z) \in \mathbb{K} \cap \mathbb{Z}^3$. Dieser Gitterpunkt liegt dann auf der Geraden

$$m := \mathbb{R}(u, v, 1) \subseteq \mathbb{K},$$

also auf der *Kegelmantellinie* durch $(u, v, 1)$. So lassen sich leicht alle Gitterpunkte von $\mathbb{K}$ finden, welche auf dieser Mantellinie liegen. Lässt man schliesslich (u, v) alle rationalen Lösungspaare von B) a) durchlaufen, so findet man alle Gitterpunkte $(x, y, z) \in \mathbb{Z}^3 \cap \mathbb{K}$ mit $z \neq 0$.

Geometrisch lässt sich die Situation wie folgt veranschaulichen (auch hier wurde $n = 2$ gewählt):

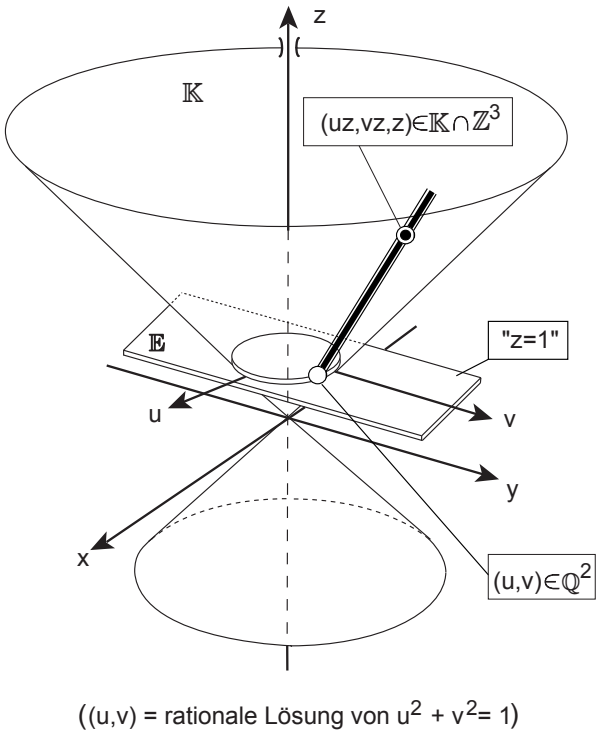


Abbildung 1.4: Lösungen von $x^2 + y^2 = z^2$ und $u^2 + v^2 = 1$

E) Nachdem wir nun den Zusammenhang zwischen den ganzzahligen Lösungen der Gleichung A) a) und den rationalen Lösungen B) a) geometrisch interpretiert haben, wollen wir die Gleichung B) a) selbst geometrisch betrachten.

Die Menge

$$\mathbb{M} := \{(u, v) \in \mathbb{R}^2 | u^n + v^n = 1\}$$

aller *reellen Lösungspaare* $(u, v) \in \mathbb{R}^2$ von B) a) bildet eine Kurve in der Ebene $\mathbb{R}^2$.

Wir betrachten diese Kurven $\mathbb{M}$ für $n = 1, 2, 3, 4$. Die Schnittpunkte von $\mathbb{M}$ mit den Koordinatenachsen nennen wir *triviale Punkte*. Sie werden mit $\circ$ markiert.

Für $n = 1$ ist $\mathbb{M}$ eine Gerade. Für $n = 2$ ist $\mathbb{M}$ ein Kreis. Ist $n \geq 3$, so nennt man $\mathbb{M}$ die *n-te Fermatkurve*. Allgemein nennt man die Lösungsmenge $\mathbb{M} \subseteq \mathbb{R}^2$ einer algebraischen Gleichung vom Grad n in zwei Unbekannten eine *Kurve vom Grad n*.
Man sagt, eine solche Kurve sei eine Quadrik, eine Kubik, eine Quartik, eine Quintik, eine Sextik, ... je nachdem, ob es sich um eine Kurve vom Grad $2, 3, 4, 5, 6, \ldots$ handelt. Entsprechend redet man von der Fermatkubik, -quartik, -quintik, -sextik, ...

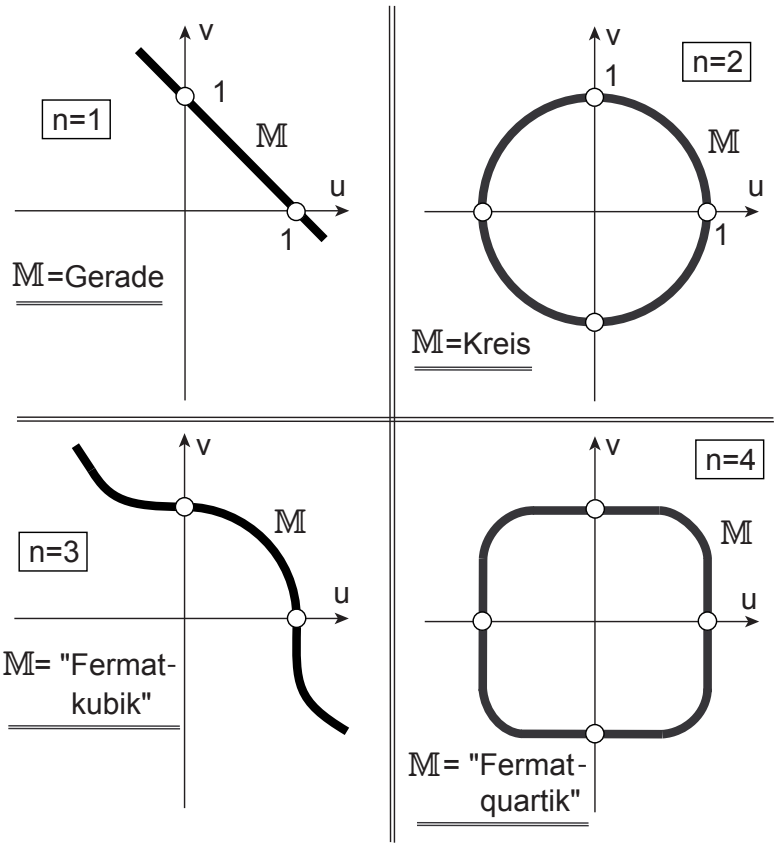


Abbildung 1.5: Lösungskurven der Gleichung $u^n + v^n = 1$

F) Sie haben sich sicher schon zur diophantischen Gleichung A) a) ihre Gedanken gemacht dabei wohl richtig festgestellt:

a) *Ist $n \geq 3$, so hat die Gleichung $x^n + y^n = z^n$ nur triviale ganzzahlige Lösungstripel (x, y, z), d.h. solche mit $xyz = 0$.*

Die Frage, ob dies wirklich so sei, geht auf Pierre de Fermat (1601–1665) zurück und hat als *grosses Fermatproblem* die Mathematik 350 Jahre lang beschäftigt. Für den Exponenten $n = 4$ wurde diese Vermutung bereits von Fermat selbst bewiesen. Im Jahre 1753 lieferte L. Euler (1707–1783) einen Beweis für den Exponenten $n = 3$. Nach immer wieder neuen Teilresultaten wurde das grosse Fermatproblem schliesslich im Jahre 1994 durch R. Taylor und A. Wiles vollständig gelöst, indem sie zeigten, dass die Aussage F) a) für jeden Exponenten $n \geq 3$ gilt. •

Bemerkung 1.8. A) Die Aussage a) aus 1.7 F) besagt, dass wir in 1.7 ausführlich über das Lösen diophantischer Gleichungen gesprochen haben, für die es in den meisten Fällen gar keine Lösung gibt. Dies erweckt den Eindruck, wir hätten in 1.7 viel Lärm um (fast) nichts gemacht.

Dieser Eindruck ist allerdings nicht richtig, denn die in 1.7 B) entwickelte Idee und die in 1.7 C), D) gezogenen geometrischen Schlussfolgerungen lassen sich auf eine grosse Klasse diophantischer Gleichungen übertragen, nämlich auf die sogenannten *homogenen diophantischen Gleichungen*. Bei diesen Gleichungen haben alle auftretenden Potenzprodukte der Unbekannten den gleichen Grad. Diesen Grad nennt man den *Grad der homogenen diophantischen Gleichung*. So ist etwa

a) $$x^3 + 3xy^2 - xyz + 7z^3 = 4yz^2$$

eine homogene Gleichung vom Grad 3 und

b) $$x^4 - xyz^2 + 11z^4 = 0$$

eine homogene Gleichung vom Grad 4.

B) Die Aussage b) aus 1.7 B) gilt nun sinngemäss für jede homogene diophantische Gleichung. Um die entsprechende Aussage zu formulieren, denken wir uns eine homogene diophantische Gleichung der Form

a) $$F(x, y, z) = 0$$

gegeben. Dazu betrachten wir auch die Gleichung

b) $$f(u, v) := F(u, v, 1) = 0,$$

welche aus a) durch umbenennen der Unbekannten und einsetzen von $z = 1$ entsteht. Dann gilt in Verallgemeinerung von 1.7 B) b) Folgendes:

c) $$\begin{cases} \textit{Sind } u, v \in \mathbb{Q} \textit{ mit } f(u, v) = 0 \textit{ und ist } z \in \mathbb{Z}\backslash\{0\} \textit{ derart, dass} \\ uz, vz \in \mathbb{Z}\textit{, so ist das Tripel } (uz, vz, z) \in \mathbb{Z}^3 \textit{ eine Lösung der} \\ \textit{homogenen diophantischen Gleichung } F(x, y, z) = 0\ . \end{cases}$$

Umgekehrt lässt sich auch hier jedes ganzzahliges Lösungstripel $(x, y, z) \in \mathbb{Z}^3$ der Gleichung a) mit $z \neq 0$ durch die in c) beschriebenen Methode finden.

C) Weil $F(x, y, z) = 0$ eine homogene Gleichung ist, gilt in den Bezeichnungen von 1.7 C) für die Menge

a) $$\mathbb{K} := \{(x, y, z) \in \mathbb{R}^3 | F(x, y, z) = 0\}$$

wieder die Aussage (vgl. 1.7 C) b)):

b) $$(x, y, z) \in \mathbb{K} \Longrightarrow \mathbb{R}(x, y, z) \subseteq \mathbb{K}.$$

Damit ist $\mathbb{K}$ auch hier wieder ein Kegel mit Spitze $(0, 0, 0)$, und die ganzzahligen Lösungen der homogenen diophantischen Gleichung B) a) sind die Gitterpunkte auf dem Kegel $\mathbb{K}$. Geometrisch besteht also auch hier eine Situation, die genau dem entspricht, was wir in 1.7 D) angetroffen haben. •

Aufgaben 1.9. A) Formulieren Sie den Satz von Taylor-Wiles als eine Aussage über die in 1.7 eingeführten Fermatkurven.

B) Zeigen Sie: Sind $a \in \mathbb{Q}\backslash\{0, 1, -1\}$ und $n \geq 3$, so ist $\sqrt[n]{1 - a^n}$ kein Bruch (*Hinweis:* A) verwenden).

C) Zeigen Sie, dass die Aussage aus B) nicht gilt, wenn $n = 2$.

D) Sei $\mathbb{M}_n$ die n-te Fermatkurve. Bestimmen Sie $a_n > 0$ so, dass $(a_n, a_n) \in \mathbb{M}_n$, und bestimmen Sie $\lim_{n\to\infty} a_n$.

E) Sei $\mathbb{M}_n$ wie in Aufgabe D). Sei $u \in]-1, 1[$. Bestimmen Sie $v_n > 0$ so, dass $(u, v_n) \in \mathbb{M}_n$. Berechnen Sie $\lim_{n\to\infty} v_n$.

F) Sei $u \in \mathbb{R}$ mit $|u| > 1$. Bestimmen Sie $w_k \in \mathbb{R}$ so, dass $(u, w_k) \in \mathbb{M}_{2k+1}$. Berechnen Sie $\lim_{k\to\infty} w_k$.

G) Skizzieren Sie den Kegel $\mathbb{K}$ aus 1.7 C) für $n = 3$ und $n = 4$ und stellen Sie die Situation entsprechend der Abbildung 1.4 dar.

H) Zeigen Sie, dass die Aussage b) aus 1.8 C) für die beiden Gleichungen 1.8 A) a), b) gilt. •

Pell'sche Gleichungen

Die diophantischen Gleichungen der Form

$$x^2 - dy^2 = 1;\ (d \in \mathbb{N}, \sqrt{d} \notin \mathbb{N})$$

heissen *Pell'sche Gleichungen*. Diese Gleichungen sind nach dem englischen Mathematiker John Pell (1610–1685) benannt, wohl fälschlicherweise: Alles deutet darauf hin, dass Pell selbst sich nicht mit diesen Gleichungen befasst hat. Die unter 8.0 d) und d') aufgeführten Gleichungen sind von diesem Typ (zumindest für die Gleichung d) besteht darüber kein Zweifel).

Bemerkungen 1.10. A) Bereits im 12. Jahrhundert beschrieb Bhaskara d. J. (1114–1191) eine allgemeine Lösungsmethode für Pell'sche Gleichungen ohne zu beweisen, dass die Methode wirklich immer zu einem Ergebnis führt. J. L. Lagrange (1736–1813) bewies im Jahre 1768, dass jede Pell'sche Gleichung unendlich viele Lösungen hat.

B) Schon Brahmagupta (598–670) kannte eine Methode, um aus einer nichttrivialen Lösung einer Pell'schen Gleichung neue Lösungen zu finden:

a) *Ist* $d \in \mathbb{N}$ *mit* $\sqrt{d} \notin \mathbb{N}$, *ist* $(x, y) \in \mathbb{N}^2$ *mit* $x^2 - dy^2 = 1$ *und ist* $n \in \mathbb{N}$, *so gibt es eindeutig bestimmte Zahlen* $x_n, y_n \in \mathbb{N}$ *mit* $x_n + y_n\sqrt{d} = (x + y\sqrt{d})^n$. *Für diese Zahlen gilt dann*

$$x_n^2 + dy_n^2 = 1;$$

d.h. (x_n, y_n) *ist wieder eine Lösung der gegebenen Pell'schen Gleichung.*

Wählt man etwa $n = 2$, so gilt $(x + y\sqrt{d})^2 = x^2 + 2xy\sqrt{d} + y^2d = (x^2 + y^2d) + (2xy)\sqrt{d}$, also $x_2 = x^2 + dy^2$ und $y_2 = 2xy$.

Gilt $x^2 - dy^2 = 1$, so folgt in der Tat

$$\begin{aligned} & x_2^2 - dy_2^2 \\ &= (x^2 + dy^2)^2 - 4dx^2y^2 \\ &= x^4 + 2dx^2y^2 + d^2y^4 - 4dx^2y^2 \\ &= x^4 - 2dx^2y^2 + d^2y^4 = (x^2 - dy^2)^2 = 1^2 = 1, \end{aligned}$$

d.h.

$$x_2^2 - dy_2^2 = 1.$$

Von Brahmagupta stammt auch die folgende Aussage:

b) *Wer innerhalb eines Jahres ein Lösungspaar* $(x, y) \in \mathbb{N}^2$ *der Gleichung*

$$x^2 - 92y^2 = 1$$

findet, ist ein(e) Mathematiker(in).

C) Ist d nicht zu gross, so lässt sich manchmal durch ausprobieren leicht die *kleinste nichttriviale Lösung* einer Pell'schen Gleichung finden (d.h. die Lösung $(x, y) \in \mathbb{N}^2$ mit kleinstem y):

Man berechnet dazu der Reihe nach die Zahlen

$$1^2, d2^2, d3^2, \ldots, dy^2, \ldots$$

und prüft jedesmal nach, ob $dy^2 + 1$ das Quadrat einer natürlichen Zahl x ist.

Ist dies der Fall, so ist $(x, y) \in \mathbb{N}^2$ eine Lösung der Gleichung $x^2 - dy^2 = 1$.

Im Fall $d = 5$ ergibt sich etwa

y	1	2	3	4	$\cdots$
$dy^2 + 1$	6	21	46	$81 = 9^2$	$\cdots$

$$\underline{\underline{9^2 - 5 \cdot 4^2 = 1}}.$$

Also ist $(9, 4)$ die kleinste nichttriviale Lösung der Pell'schen Gleichung $x^2 - 5y^2 = 1$.

D) Die Menge

a) $$\mathbb{H} := \{(x, y) \in \mathbb{R}^2 | x^2 - dy^2 = 1\}$$

aller *reellen Lösungspaare* (x, y) der Pell'schen Gleichung $x^2 - dy^2 = 1$ bildet eine Hyperbel mit den Scheitelpunkten $(1, 0)$ und $(-1, 0)$ und den Asymptoten $y = \pm\sqrt{d}^{-1}x$. Die ganzzahligen Lösungen dieser Gleichung sind also gerade die Gitterpunkte auf der Hyperbel $\mathbb{H}$:

b) $$\{(x, y) \in \mathbb{Z}^2 | x^2 - dy^2 = 1\} = \mathbb{Z}^2 \cap \mathbb{H}.$$

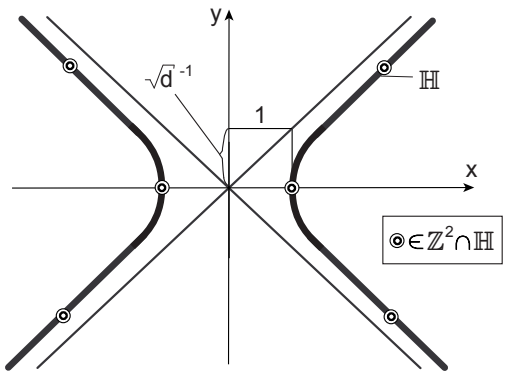


Abbildung 1.6: Lösungskurve einer Pell'schen Gleichung

•

Aufgaben 1.11. A) Bestimmen Sie die minimalen Lösungen der folgenden Pell'schen Gleichungen:

$$x^2 - 2y^2 = 1,\ x^2 - 3y^2 = 1,\ x^2 - \ 7y^2 = 1,$$
$$x^2 - 6y^2 = 1,\ x^2 - 8y^2 = 1,\ x^2 - 10y^2 = 1.$$

B) Sei $d \in \mathbb{N}$ mit $\sqrt{d} \notin \mathbb{N}$. Seien $x, y, x', y' \in \mathbb{N}$ so, dass $x + y\sqrt{d} = x' + y'\sqrt{d}$. Zeigen Sie, dass $x = x'$ und $y = y'$ (*Hinweis:* 2.8 beachten).

C) Sei $d \in \mathbb{N}$ mit $\sqrt{d} \notin \mathbb{N}$ und sei $(x, y) \in \mathbb{N}^2$ mit $x^2 - dy^2 = 1$. Wir definieren die Paare $(x_n, y_n) \in \mathbb{N}^2$ $(n = 1, 2, 3, \ldots)$ durch

$$x_n = \begin{cases} x, & \text{falls } n = 1; \\ xx_{n-1} + dyy_{n-1}, & \text{falls } n > 1, \end{cases};$$
$$y_n = \begin{cases} y, & \text{falls } n = 1; \\ xy_{n-1} + x_{n-1}y, & \text{falls } n > 1. \end{cases}$$

Zeigen Sie durch Induktion über n:

a) $x_n^2 - dy_n^2 = 1$.

b) $x_n + y_n\sqrt{d} = (x + y\sqrt{d})^n$.

c) $x_n - y_n\sqrt{d} = (x - y\sqrt{d})^n$.

D) Sei $d \in \mathbb{N}$ so, dass $d + 2$ das Quadrat einer natürlichen Zahl ist. Zeigen Sie, dass das Paar $\left(d + 1, \sqrt{d + 2}\right)$ eine Lösung der Pell'schen Gleichung $x^2 - dy^2 = 1$ ist.

E) Wenden Sie D) mit $d = 23$ und dann C) mit $n = 2$ an um zu zeigen, dass Sie ein(e) Mathematiker(in) sind.

F) Sei $d \in \mathbb{N}$ mit $\sqrt{d} \notin \mathbb{N}$. Zeigen Sie:

Ist $(x, y) \in \mathbb{N}^2$ eine Lösung der Pell'schen Gleichung $x^2 - dy^2 = 1$, so gilt

$$x = \min\left\{ n \in \mathbb{N} \,\middle|\, n > \sqrt{d}y \right\}.$$

G) Versuchen Sie (z. B. im Internet) ausfindig zu machen, worin der Ruhm der Gleichung 8.0 d') bestehen könnte und berichten Sie kurz über das Gefundene.

H) Beweisen Sie ohne Rechner und nur unter Verwendung der letzten drei Ziffern im Zahlkoeffizienten der Gleichung 1.0 d'), dass diese Gleichung wirklich eine Pell'sche Gleichung ist (*Hinweis:* Durch 8 teilen!).

I) Geben Sie jeweils 3 verschiedene nichttriviale Lösungspaare $(x, y) \in \mathbb{N}^2$ der Pell'schen Gleichungen

$$x^2 - 14y^2 = 1, \; x^2 - 34y^2 = 1$$

an. (*Hinweis:* Aufgaben C), E).)

J) (*Square-Town*) Ein quadratisches Wohnquartier besteht aus lauter gleich grossen quadratischen Parzellen. Zwei Parzellen werden als Spielplatz genutzt. Auf jeder anderen Parzelle steht ein Einfamilienhaus, von denen jedes einen quadratischen Sitzplatz hat. Dabei sind alle Sitzplätze gleich gross. Zwischen dem Wohnquartier und dem in ca. 45 m Entfernung vorbeifliessenden Fluss befindet sich ein quadratischer Parkplatz, der eine unwesentlich grössere Fläche hat als alle Sitzplätze zusammen (Unterschied weniger als 0.2m^2. Alle Plätze sind mit ganzen quadratischen Platten der Grösse $40\text{cm} \times 40\text{cm}$ belegt. Auf jedem Sitzplatz liegen gleichviele Platten wie es im Quartier Parzellen hat.

Wie viele Häuser stehen höchstens im Quartier?

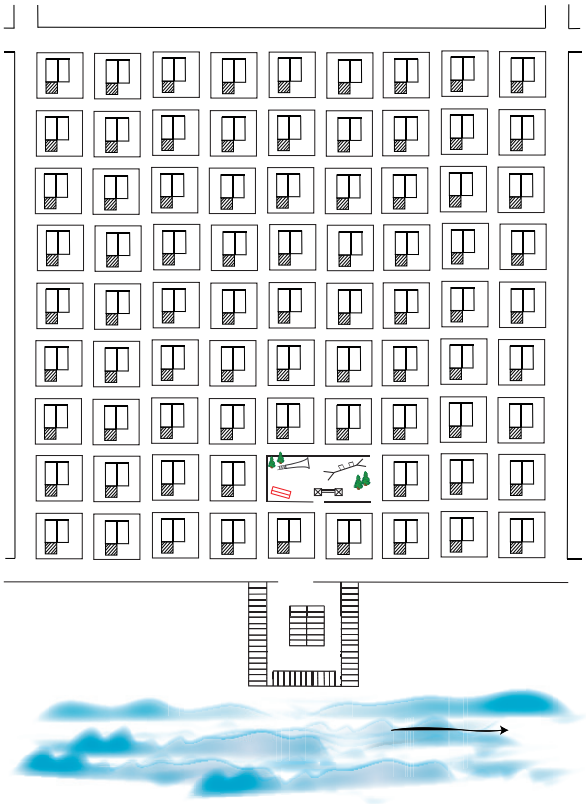


Abbildung 1.7: Square-Town

•

Kapitel 2

Homogene quadratische Gleichungen

Überblick

Wir beginnen dieses Kapitel mit der Bestimmung der sogenannten *pythagoräischen Tripel*. Wir greifen dazu auf die in 1.7 gemachte Beobachtung zurück, dass es dazu genügt, die rationalen Punkte auf dem Einheitskreis „zu bestimmen“. Zur Bestimmung dieser rationalen Punkte verwenden wir die Idee der „*rationalen Parametrisierung des Einheitskreises*“. In Tat und Wahrheit könnten wir die pythagoräischen Tripel auch ohne dieses geometrische Hilfsmittel bestimmen. Doch dann würde uns der schöne Zusammenhang zwischen der Arithmetik und der Geometrie entgehen, der für eine grössere Klasse von diophantischen Gleichungen besteht: Alle Lösungen einer sogenannten *(nichtausgearteten) homogenen quadratischen diophantischen Gleichung* lassen sich mit Hilfe einer geometrischen Methode aus einer einzigen nichttrivialen Lösung berechnen, und das mit Hilfe einer rationalen Parametrisierung.

Das Lösen (nichtausgearteter) homogener quadratischer diophantischer Gleichungen zerfällt also in zwei Teilschritte:

- Entscheiden, ob eine nichttriviale Lösung existiert und bestimmen einer solchen;
- Explizite Beschreibung aller Lösungen mit Hilfe der im ersten Schritt bestimmen Einzellösung.

Der erste Teilschritt ist rein arithmetischer Art und beruht auf einer Methode, die wir im Rahmen dieser Vorlesung nicht behandeln können – dem sogenannten *Hasseprinzip*.

Der zweite Teilschritt beruht auf der geometrischen Idee der *rationalen Parametrisierung von Quadriken*. Eine detaillierte Behandlung dieser Methode würde den Rahmen dieses Kapitels allerdings sprengen. Wir verlegen dieses Thema deshalb ins nächste Kapitel.

Trotzdem wollen wir uns unentwegt daran machen, die im Titel genannten Gleichungen zu behandeln. Im einzelnen kommen folgende Themen zur Sprache:

- *Pythagoräische Tripel,*
- *Rationale Parametrisierung des Einheitskreises,*
- *Bestimmung der phythagoräischen Tripel,*
- *Von der Geometrie zur Arithmetik: ein Rückblick,*
- *Homogene quadratische diophantische Gleichungen,*
- *Zur Existenz nichttrivialer Lösungen.*

Pythagoräische Tripel

Wir befassen uns als erstes mit den sogenannten *pythagoräischen Tripeln*, d.h. mit den nichttrivialen Lösungen der diophantischen Gleichung $x^2 + y^2 = z^2$. Das Ziel ist schliesslich die Bestimmung aller dieser Tripel und zwar auf dem geometrischen Weg der rationalen Parametrisierung, der schon oben genannt wurde. Zunächst machen wir allerdings eine allgemeine Vorbetrachtung über pythagoräische Tripel.

Definition und Bemerkung 2.1. A) Ein *pythagoräisches Tripel* ist ein Tripel $(x, y, z) \in \mathbb{N}^3$ natürlicher Zahlen so, dass $x^2 + y^2 = z^2$.

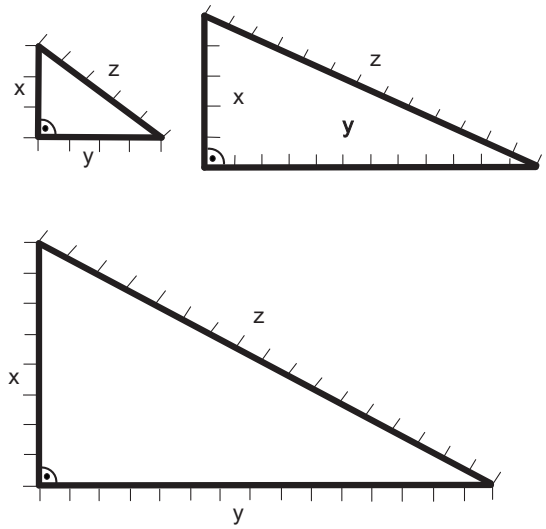


Abbildung 2.1: Pythagoräische Tripel

B) Schon in der Antike hat man nach der Menge aller pythagoräischen Tripel gesucht, und Diophantos hat zu diesem Problem die Lösung gefunden. Wir wollen dieses Problem nochmals im Lichte der Bemerkung 1.7 betrachten.

Es geht also darum, alle Lösungstripel $(x, y, z) \in \mathbb{Z}^3$ der diophantischen Gleichung $x^2 + y^2 = z^2$ (d.h. der Gleichung a) aus 1.7 A) mit $n = 2$) zu finden, die zudem noch der Nebenbedingung $0 < x \leq y \leq z$ genügen sollen. Ist $(x, y, z) \in \mathbb{Z}^3$ ein Lösungstripel mit $x, y, z \neq 0$, so lässt sich durch Vorzeichenwechsel und allfälliges Vertauschen von x und y ein Lösungstripel gewinnen, das unserer Nebenbedingung genügt. Wenn wir im Moment die Nebenbedingung ausser acht lassen, geht es somit genau um das Lösen der diophantischen Gleichung $x^2 + y^2 = z^2$. Nach 1.7 B) sind wir also mit dem Problem konfrontiert, die *rationalen Punkte auf dem Einheitskreis*

$$\mathbb{M} = \{(u, v) \in \mathbb{R}^2 | u^2 + v^2 = 1\}$$

„zu bestimmen“. •

Aufgaben 2.2. A) Interpretieren Sie diese antike Werbeanzeige.

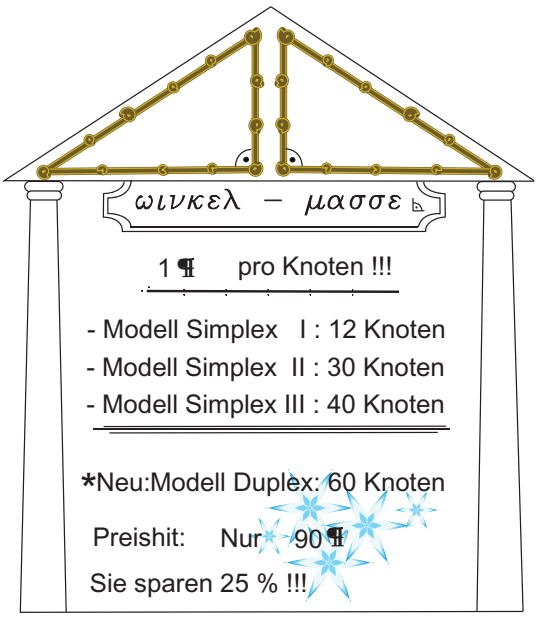


Abbildung 2.2: Antike Werbeanzeige

B) Sei $(x, y, z) \in \mathbb{N}^3$ ein pythagoräisches Tripel. Zeigen Sie die folgende Implikation: $x \in \mathbb{P} \Longrightarrow y = \frac{x^2-1}{2} \wedge z = \frac{x^2+1}{2}$. (*Hinweis:* Schreiben Sie $x^2 = \ldots$).

C) Sei $(x, y, z) \in \mathbb{N}^3$ ein pythagoräisches Tripel mit $x \leq y$. Zeigen Sie, dass $x < y$ und $y \notin \mathbb{P}$.

D) Zeigen Sie, dass es zu jedem ungeraden $x \in \mathbb{N}_{\geq 3}$ genau ein pythagoräisches Tripel (x, y, z) gibt, für welches $z = y + 1$ gilt. Drücken Sie y und z durch x aus.

E) Zeigen Sie, dass es unendlich viele pythagoräische Tripel (x, y, z) so gibt, dass $z = y+1$ gilt und dass z eine Quadratzahl ist (*Hinweis:* z durch x ausdrücken, 1.10 A) oder – noch besser – 1.10 B) a) resp. 1.11 C), D) verwenden). •

Rationale Parametrisierung des Einheitskreises

Jetzt fhren wir das shcon früher genannte geometrische Hilfsmittel ein, welches erlaubt, die rationalen Punkte auf dem Einheitskreis „zu bestimmen“, d.h. in befriedigender Weise zu beschreiben. Es handelt sich dabei um eine sogenannte *rationale Parametrisierung des Einheitskreises*.

Konstruktion 2.3. (vgl. 1.7 A)) A) Wir betrachten den Einheitskreis

$$\mathbb{M} = \{(u, v) \in \mathbb{R}^2 | u^2 + v^2 - 1 = 0\}.$$

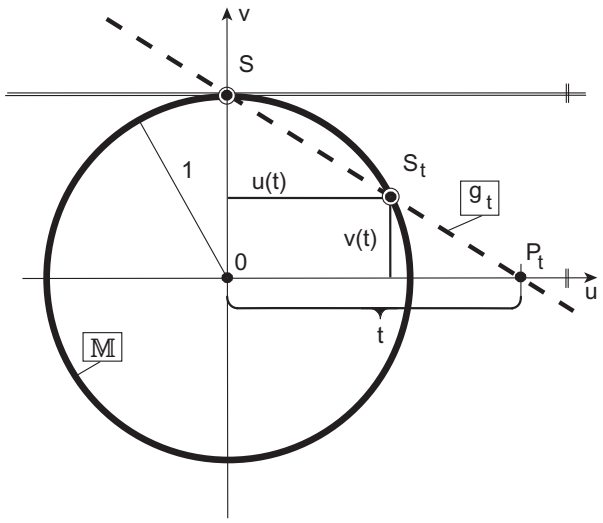


Abbildung 2.3: Parametrisierung des Einheitskreises

Dann wählen wir einen „Parameterwert“ $t \in \mathbb{R}$ und betrachten die Gerade g_t, welche die beiden Punkte

$$P_t := (t, 0) \text{ und } S := (0, 1)$$

verbindet. Die Gerade g_t schneidet $\mathbb{M}$ in S und einem weiteren Punkt S_t. Die Koordinaten von S_t bezeichnen wir mit $u(t)$ und $v(t)$, also

$$S_t = (u(t), v(t)) \,; \mathbb{M} \cap g_t = \{S, S_t\}.$$

Die Gerade g_t hat die Parameterdarstellung

$$s \mapsto \overrightarrow{0S} + s\overrightarrow{SP_t} = (0,1) + s(t,-1) = (st, 1-s).$$

Um S_t zu suchen, muss man s so wählen, dass $(st, 1-s) \in \mathbb{M}$. Dies führt zur Gleichung

$$(st)^2 + (1-s)^2 - 1 = 0.$$

Die linke Seite dieser Gleichung lässt sich schreiben als

$$s^2t^2 + 1 - 2s + s^2 - 1 = s^2t^2 + s^2 - 2s = s\left(s(t^2+1) - 2\right).$$

So erhalten wir die Gleichung

$$s\left(s(t^2+1) - 2\right) = 0.$$

Diese Gleichung hat die beiden Lösungen

$$s = 0 \text{ und } s = \frac{2}{t^2+1}.$$

Für $s = 0$ erhalten wir den Schnittpunkt S. Für $s = \frac{2}{t^2+1}$ erhalten wir also den Schnittpunkt $S_t = (u(t), v(t))$. Einsetzen von $s = \frac{2}{t^2+1}$ in die Parameterdarstellung a) liefert demnach

$$(u(t), v(t)) = S_t = \left(\frac{2t}{t^2+1}, 1 - \frac{2}{t^2+1}\right) = \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right),$$

d.h.

$$u(t) = \frac{2t}{t^2+1} \text{ und } v(t) = \frac{t^2-1}{t^2+1}.$$

(Die geometrische Überlegung aus der Musterlösung zu 1.7 hat mit andern Bezeichnungen das Gleiche geliefert.)

B) Insbesondere besteht nun eine Abbildung

$$\varepsilon : \mathbb{R} \to \mathbb{M}\backslash\{S\},\ t \mapsto \varepsilon(t) := (u(t), v(t)) = \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right).$$

Schon aus der geometrischen Situation ist klar, dass ε bijektiv ist. Um diese Bijektivität rein algebraisch zu zeigen, kann man aber auch die Abbildung

$$\iota : \mathbb{M}\backslash\{S\} \to \mathbb{R},\ (u,v) \mapsto \iota(u,v) := \frac{u}{1-v}$$

einführen und nachrechnen, dass ι die Umkehrabbildung von ε ist, d.h. dass

a) $$\iota(\varepsilon(t)) = t \text{ für alle } t \in \mathbb{R} \text{ und}$$

b) $$\varepsilon(\iota(u,v)) = (u,v) \text{ für alle } (u,v) \in \mathbb{M}\backslash\{S\}.$$

Die Abbildung ε ist eine sogenannte *rationale Parametrisierung von* $\mathbb{M}$ (genauer von $\mathbb{M}\backslash\{S\}$), da ihre Komponentenfunktionen $u(t)$ und $v(t)$ rationale Funktionen sind.

C) Schliesslich wollen wir uns überlegen, dass für eine reelle Zahl $t \in \mathbb{R}$ die folgende Äquivalenz besteht:

$$t \in \mathbb{Q} \Longleftrightarrow \varepsilon(t) \in \mathbb{Q}^2.$$

Wegen $\varepsilon(t) = \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right)$ ist die Implikation „$\Longrightarrow$“ sofort klar. Ist umgekehrt $\varepsilon(t) = (u,v) \in \mathbb{Q}^2$, so gilt $t = \iota(\varepsilon(t)) = \iota(u,v) = \frac{u}{1-v} \in \mathbb{Q}$.

Damit ist aber gezeigt:

- *Durch Einschränken von ε erhält man eine bijektive Abbildung*

$$\varepsilon\restriction: \mathbb{Q} \to \mathbb{Q}^2 \cap (\mathbb{M}\backslash\{S\}),\ t \mapsto \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right).$$

Die Abbildung $\varepsilon\restriction$ liefert also eine *Parametrisierung von* $\mathbb{Q}^2 \cap (\mathbb{M}\backslash\{S\})$ *durch die Menge* $\mathbb{Q}$ *der rationalen Zahlen.* Wir sprechen auch von einer *Parametrisierung der rationalen Punkte auf* $\mathbb{M}$ oder einer *Parametrisierung der rationalen Lösungen der Gleichung* $u^2 + v^2 - 1 = 0$.

Insbesondere lässt sich die *Menge* $\mathbb{Q}^2 \cap \mathbb{M}$ *der rationalen Punkte auf* $\mathbb{M}$ einfach beschreiben:

a) $$\mathbb{Q}^2 \cap \mathbb{M} = \varepsilon(\mathbb{Q}) \cup \{S\} = \left\{ \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right) \middle| t \in \mathbb{Q} \right\} \cup \{(0,1)\}.$$

•

Aufgaben 2.4. A) Wir betrachten den Einheitskreis

$$\mathbb{M} = \{(u,v) \in \mathbb{R}^2 | u^2 + v^2 - 1 = 0\}$$

und die Abbildung (d.h. die Parametrisierung von $\mathbb{M}$)

$$\varphi : \mathbb{R} \to \mathbb{M},\ \alpha \mapsto (\cos(\alpha), \sin(\alpha)).$$

Bestimmen Sie $\varphi^{-1}(u,v)$ für einen beliebigen Punkt $(u,v) \in \mathbb{M}$.

B) Es gelten die Bezeichnungen von A). Zeigen Sie, dass die Menge $\mathbb{S} := \varphi^{-1}(\mathbb{Q}^2 \cap \mathbb{M})$ folgende Eigenschaften hat:

a) $0 \in \mathbb{S}$;

b) $\alpha \in \mathbb{S} \Rightarrow -\alpha \in \mathbb{S}$;

c) $\alpha, \beta \in \mathbb{S} \Rightarrow \alpha + \beta \in \mathbb{S}$, (*Hinweis:* Additionstheoreme);

d) $\alpha \in \mathbb{S}, n \in \mathbb{Z} \Rightarrow \alpha + 2n\pi \in \mathbb{S}$.

C) Rechnen Sie nach, dass die Aussagen c) und d) aus 2.3 B) tatsächlich gelten.

D) Skizzieren Sie auf dem Einheitskreis die Punkte $\varepsilon(0), \varepsilon(1), \varepsilon(2), \varepsilon(3), \ldots$ und bestimmen Sie $\lim_{n\to\infty} \varepsilon(n)$ (vgl. 2.3).

E) Zeigen Sie, dass $(2n, n^2 - 1, n^2 + 1)$ für jedes $n \in \mathbb{N}_{\geq 2}$ ein pythagoräisches Tripel ist.

•

Bestimmung der pythagoräischen Tripel

Mit Hilfe der oben beschriebenen *Parametrisierung der rationalen Lösungen der Gleichung* $u^2 + v^2 - 1 = 0$ wollen wir nun pythagoräische Tripel $(x, y, z) \in \mathbb{N}^3$ bestimmen.

Bemerkungen und Definition 2.5. A) Seien $m, n \in \mathbb{N}$. Wir wollen uns überlegen:

a) *Sind* m *und* n *ungerade, so gelten* $m^2+n^2 \equiv 2 \mod (4)$ *und* $m^2-n^2 \equiv 0 \mod (4)$.

In der Tat gelten mit geeigneten Zahlen $k, l \in \mathbb{Z}$ die Gleichungen $m = 2k + 1$ und $n = 2l + 1$, und es folgen

$$m^2 + n^2 = (2k + 1)^2 + (2l + 1)^2 = 4(k^2 + l^2 + k + l) + 2,$$
$$m^2 - n^2 = (2k + 1)^2 - (2l + 1)^2 = 4(k^2 + l^2 + k - l).$$

B) Sei $z \in \mathbb{N}$. Dann gilt $z^2 \not\equiv 2 \bmod(4)$, was man sich wie folgt überlegt: Falls z ungerade ist, so ist es auch z^2, und es folgt $z^2 \not\equiv 2 \bmod(4)$. Ist z gerade, so gilt $z = 2n$ für ein geeignetes $n \in \mathbb{N}$. Damit erhalten wir aber $z^2 = 4n^2 \equiv 0 \bmod(4) \not\equiv 2 \bmod(4)$. Aus der ersten Kongruenz in A) a) folgt damit sofort:

a) *Ist* (x, y, z) *ein pythagoräisches Tripel, so ist mindestens eine der Zahlen* x *oder* y *gerade.*

C) Ein *primitives pythagoräisches Tripel* ist ein pythagoräisches Tripel (x, y, z) so, dass

$$\mathrm{ggT}(x, y) = 1 \text{ und } 2|x.$$

Für ein solches Tripel (x, y, z) gelten offenbar

a) $$2 \nmid y \text{ und } \mathrm{ggT}(x, z) = \mathrm{ggT}(y, z) = 1.$$

D) Ein beliebiges pythagoräisches Tripel (x, y, z) entsteht immer, indem in einem geeigneten primitiven pythagoräischen Tripel (x_0, y_0, z_0) alle Komponenten mit einer geeigneten Zahl $k \in \mathbb{N}$ multipliziert und dann allenfalls noch die ersten beiden Komponenten vertauscht werden:

Ist nämlich $k = \mathrm{ggT}(x, y)$, so folgt $k^2|(x^2 + y^2) = z^2$, also $k|z$. Mit geeigneten Zahlen $x_0, y_0, z_0 \in \mathbb{N}$ gelten also $x = kx_0, y = ky_0$ und $z = kz_0$, und wegen $k^2(x_0^2+y_0^2) = x^2+y^2 = z^2 = k^2z_0^2$ ist (x_0, y_0, z_0) wieder ein pythagoräisches Tripel. Dabei ist $\mathrm{ggT}(x_0, y_0) = 1$. Gemäss Aussage B) a) können wir nach allfälligem Vertauschen von x_0 und y_0 annehmen, es gelte $2|x_0$. •

Nun können wir die angekündigte Charakterisierung der pythagoräischen Tripel vornehmen.

Satz 2.6. *(Satz von Diophantos) Die primitiven pythagoräischen Tripel sind genau die Tripel der Form*

$$(2mn, m^2 - n^2, m^2 + n^2) \in \mathbb{N}^3$$

mit $m, n \in \mathbb{N}$ *so, dass*

$$n < m,\ \mathrm{ggT}(m, n) = 1,\ m \not\equiv n \bmod(2).$$

Beweis: Sind $x = 2mn$, $y = m^2-n^2$ und $z = m^2+n^2$ mit $m, n \in \mathbb{N}$ wie im Satz verlangt, so haben x, y, z sicher keinen gemeinsamen Teiler. Denn ein gemeinsamer Primfaktor von $x = 2mn$ und $y = m^2 - n^2$ müsste ein gemeinsamer Faktor von m und n oder aber 2 sein. Beides ist nach Voraussetzung ausgeschlossen.

Zudem gilt $x^2 + y^2 = (2mn)^2 + (m^2 - n^2)^2 = m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2 = z^2$. Also ist (x, y, z) ein primitives pythagoräisches Tripel.

Sei nun umgekehrt $(x, y, z) \in \mathbb{N}^3$ ein primitives pythagoräisches Tripel. Seien $u = \frac{x}{z}$ und $v = \frac{y}{z}$. Dann ist (u, v) ein rationaler Punkt auf dem Einheitskreis $\mathbb{M}$. Wegen $x \neq 0$ ist $u \neq 0$, also $(u, v) \neq (0, 1)$. Nach 2.3 C) a) gibt es also ein $t \in \mathbb{Q}$ mit

$$u = \frac{2t}{t^2 + 1}, \quad v = \frac{t^2 - 1}{t^2 + 1}.$$

Wegen $u > 0$ und $v > 0$ ist klar, dass $t > 1$. Wir können also schreiben:

$$t = \frac{m}{n} \text{ mit } m, n \in \mathbb{N},\ n < m,\ \mathrm{ggT}(m, n) = 1.$$

Es folgen:

$$u = \frac{2\frac{m}{n}}{\frac{m^2}{n^2} + 1} = \frac{2mn}{m^2 + n^2}; \quad v = \frac{\frac{m^2}{n^2} - 1}{\frac{m^2}{n^2} + 1} = \frac{m^2 - n^2}{m^2 + n^2}.$$

Wegen $u = \frac{x}{z}$ und $v = \frac{y}{z}$ erhalten wir

$$(\alpha) \qquad x(m^2 + n^2) = 2mnz;$$

$$(\beta) \qquad y(m^2 + n^2) = (m^2 - n^2)z.$$

Wir wollen als nächstes zeigen, dass $m \not\equiv n \mod (2)$. Nehmen wir an, es sei $m \equiv n \mod (2)$, also $2|(m - n)$. Weil m und n teilerfremd sind, müssen dann beide ungerade sein. Nach 2.5 A) a) folgen $4|(m^2 - n^2)$ und $4 \nmid (m^2 + n^2)$. Mit (β) ergibt sich daraus $2|y$, also ein Widerspruch zu 2.5 C) a). Deshalb ist $m \not\equiv n \mod(2)$.

Insbesodere ist eine der beiden Zahlen m oder n ungerade, die andere aber gerade. Deshalb gilt $2 \nmid (m^2 + n^2)$. Dies zieht aber nach sich, dass

$$(\gamma) \qquad \mathrm{ggT}(m^2 + n^2, 2mn) = 1,$$

denn ein gemeinsamer Primfaktor von $m^2 + n^2$ und $2mn$ wäre ja ein Primfaktor von $m^2 + n^2$ und mn, was der Teilerfremdheit von m und n widerspräche.

Aus den Gleichungen (α) und (γ) ergibt sich $(m^2 + n^2)|z$.

Weil x und z teilerfremd sind (s. 2.5 C) a)), folgt aus Gleichung (α) auch $z|(m^2 + n^2)$. Damit wird $z = m^2 + n^2$ und die Gleichungen (α) und (β) liefern $x = 2mn, y = m^2 - n^2$. ■

Aufgaben 2.7. A) Ist (x, y, z) ein pythagoräisches Tripel, so nennen wir $x + y + z$ den *Umfang* dieses Tripels. Zeigen Sie, dass eine Zahl $u \in \mathbb{N}$ genau dann der Umfang eines primitiven pythagoräischen Tripels ist, wenn gilt:

$$u = 2mk,\ \text{mit } m, k \in \mathbb{N}, m < k < 2m,\ k \text{ ungerade und } \mathrm{ggT}(m, k) = 1.$$

B) Sei $v \in \mathbb{N} \setminus \{1\}$ und sei $\mathring{\mathbb{T}}(v) := \{w \in \mathbb{T}(v) | \mathrm{ggT}(w, \frac{v}{w}) = 1\}$ (vgl. **??** H)). Zeigen Sie, dass die Anzahl primitiver pythagoräischer Tripel vom Umfang $u := 2v$ gegeben ist durch

$$\lambda(u) := \sharp \left\{ m \in \mathring{\mathbb{T}}(v) \setminus \{1, v\} \,\middle|\, \frac{v}{2} < m^2 < v \wedge 2^{\nu_2(v)} | m \right\}.$$

C) Zeigen Sie, dass eine Zahl $u \in \mathbb{N}$ genau dann der Umfang eines pythagoräischen Tripels ist, wenn $u = 2mkl$, wobei $m, k, l \in \mathbb{N}$ und m und k den Bedingungen aus Teil A) genügen. Schliessen Sie, dass die Anzahl pythagoräischer Tripel vom Umfang u gegeben ist durch $\lambda(u) := \sum_{2|w|u} \lambda(w)$.

D) Sei u das Produkt der ersten 8 Primzahlen. Wie viele pythagoräische Tripel mit Umfang u gibt es?

E) Für jedes $n \in \mathbb{N}_{\geq 2}$ sei (x_n, y_n, z_n) ein primitives pythagoräisches Tripel mit Umfang $2^n(2^{n-1}+1)$. Bestimmen Sie dieses Tripel und berechnen Sie

$$\lim_{n\to\infty} \frac{y_n}{x_n}, \ \lim_{n\to\infty} \frac{z_n}{x_n} \text{ und } \lim_{n\to\infty} \frac{z_n}{y_n}.$$

F) Sei $\mathbb{H} := \{(x, y, z) \in \mathbb{Z}^3 \backslash \{(0, 0, 0)\} | x^2 + y^2 = z^2\}$. Zeigen Sie:

$$(x, y, z), (x', y', z') \in \mathbb{H} \Longrightarrow (xx' - yy', xy' + x'y, zz') \in \mathbb{H}.$$

G) Gemäss F) können wir auf $\mathbb{H}$ eine Verknüpfung „$\oplus$“ definieren durch

$$(x, y, z) \oplus (x', y', z') := (xx' - yy', xy' + x'y, zz').$$

Zeigen Sie, dass diese Verknüpfung assoziativ und kommutativ ist und das Neutralelement $(1, 0, 1)$ hat. •

Von der Geometrie zur Arithmetik: ein Rückblick

Mit 2.6 haben wir ein klassisches Problem der Arithmetik gelöst: die Bestimmung aller (primitiven) pythagoräischen Tripel, d.h. die Bestimmung aller (nichttrivialen) Lösungen der diophantischen Gleichung $x^2 + y^2 - z^2 = 0$.

Als wesentliches Hilfsmittel haben wir gebraucht, dass die Parametrisierung ε aus 2.3 zu jeder rationalen Zahl t ein Lösungstripel $(x(t), y(t), z(t)) \in \mathbb{Z}^3 \backslash \{(0, 0, 0)\}$ unserer Gleichung liefert. Diese Idee, mit Hilfe der Geometrie ein arithmetisches Problem zu lösen, ist aber so wichtig, dass wir sie im folgenden nochmals rekapitulieren. Im dritten Kapitel werden wir dann schliesslich “den Faden in dieser Richtung weiterspinnen”.

Bemerkung 2.8. A) Wir setzen

$$F(x, y, z) := x^2 + y^2 - z^2$$

und interessieren uns für die Tripel $(x, y, z) \in \mathbb{Z}^3 \backslash \{(0, 0, 0)\}$ mit $F(x, y, z) = 0$, also für die Menge

$$\mathbb{L}(F) := \left\{ (x, y, z) \in \mathbb{Z}^3 \backslash \{(0, 0, 0)\} \middle| \, F(x, y, z) = 0 \right\}.$$

Für jedes Tripel $(x, y, z) \in \mathbb{L}(F)$ muss natürlich $z \neq 0$ gelten. Wir können also

$$\mathbb{L}_z(F) := \{(x, y, z) \in \mathbb{L}(F) | z \neq 0\}$$

schreiben und haben dann $\mathbb{L}_z(F) = \mathbb{L}(F)$. Es genügt deshalb, dass wir $\mathbb{L}_z(F)$ bestimmen. Offensichtlich gilt

$$(x_0, y_0, z_0) := (0, 1, 1) \in \mathbb{L}_z(F).$$

Aus diesem einen Tripel in $\mathbb{L}_z(F)$ lassen sich nun alle andern wie folgt finden:

B) Wir betrachten das quadratische Polynom in u und v, das gegeben ist durch (vgl. 2.3)

$$f(u, v) := F(u, v, 1) = u^2 + v^2 - 1,$$

sowie die Menge

$$\mathbb{M}(f) := \left\{(u, v) \in \mathbb{R}^2 | f(u, v) = 0\right\} = \mathbb{M}$$

und den Punkt

$$S = (u_0, v_0) := \left(\frac{x_0}{z_0}, \frac{y_0}{z_0}\right) = (0, 1) \in \mathbb{Q}^2 \cap \mathbb{M}.$$

Dann betrachten wir die rationale Parametrisierung

$$\varepsilon : \mathbb{R} \longrightarrow \mathbb{M}\backslash\{S\};\ t \mapsto \varepsilon(t) := (u(t), v(t))$$

aus 2.3 B) und die aus dieser resultierende Beziehung (vgl. 2.3 C))

a) $$\mathbb{Q}^2 \cap \mathbb{M} = \varepsilon(\mathbb{Q}) \cup \{S\} = \{(u(t), v(t)) \,| t \in \mathbb{Q}\} \cup \{(u_0, v_0)\}\,.$$

C) Nun haben wir alle rationalen Punkte von $\mathbb{M}$ in geschlossener Form dargestellt und können jetzt 1.7 anwenden um alle ganzzahligen Lösungen der Gleichung $F(x, y, z) = 0$ (mit $z \neq 0$) zu bestimmen. Wir wollen auch diesen letzten Schritt nochmals rekapitulieren. Dazu führen wir zunächst eine geeignete Bezeichnungsweise ein.

Sind $u, v \in \mathbb{Q}$, so stehe $\eta(u, v)$ für den *kleinsten gemeinsamen Nenner von u und v*, also

$$\eta(u, v) := \min\{n \in \mathbb{N} | nu, nv \in \mathbb{Z}\}$$

oder, in der Bezeichnungsweise von 2.6:

a) $$\eta(u, v) = \mathrm{kgV}\,(\eta(u), \eta(v))\,.$$

Ist $z \in \mathbb{Z}\backslash\{0\}$, so kann man sagen:

$$zu, zv \in \mathbb{Z} \Longleftrightarrow \eta(u, v) | z.$$

Nun liefert die Aussage 1.7 B) b) sofort

$$\mathbb{L}_z(F) = \left\{(zu, zv, z) \,\middle|\, (u, v) \in \mathbb{Q}^2 \cap \mathbb{M}, z \in \mathbb{Z}\eta(u, v)\backslash\{0\}\right\},$$

und mit der obigen Aussage B) a) folgt

$$\mathbb{L}_z(F) = \{(zu(t), zv(t), z) | t \in \mathbb{Q}, z \in \mathbb{Z}\eta(u(t), v(t))\backslash\{0\}\}$$
$$\cup \{(\lambda x_0, \lambda y_0, \lambda z_0) | \lambda \in \mathbb{Z}\backslash\{0\}\}.$$

Da man zu jedem $t \in \mathbb{Q}$ leicht die rationalen Zahlen $u(t), v(t)$ und deren gemeinsamen Nenner $\eta(u(t), v(t))$ bestimmen kann, liefert diese Aussage eine gute Beschreibung der Lösunsmenge $\mathbb{L}_z(F)$. •

Aufgaben 2.9. A) Seien $u(t)$ und $v(t)$ wie in 2.3. Bestimmen Sie zu jedem pythagoräischen Tripel (x, y, z) vom Umfang kleiner oder gleich 60 einen positiven Bruch t so, dass $(x, y, z) = (zu(t), zv(t), z)$.

B) Es gelten die Bezeichnungen von A). Bestimmen Sie vier positive Brüche t_1, t_2, t_3, t_4 so, dass $\eta(u(t_1), v(t_1)) < \eta(u(t_2), v(t_2)) < \eta(u(t_3), v(t_3)) < \eta(u(t_4), v(t_4))$ und dass die Zahl $\eta(u(t_4), v(t_4))$ möglichst klein wird.

C) Sei $t \in \mathbb{Q}_{\geq 0}\backslash\{1\}$. Bestimmen Sie eine Zahl $s \in \mathbb{Q}_{\geq 0}\backslash\{t\}$ so, dass $\eta(u(s), v(s)) = \eta(u(t), v(t))$. Begründen oder interpretieren Sie das Ergebnis geometrisch. •

Homogene quadratische diophantische Gleichungen

Die in 2.8 beschriebene Lösungsidee für die diophantische Gleichung $x^2 + y^2 - z^2 = 0$ lässt sich auf eine grössere Klasse diophantischer Gleichungen $F(x, y, z) = 0$ übertragen: auf die sogenannten (nichtausgearteten) *homogenen quadratischen diophantischen Gleichungen*. Zu dieser Klasse diophantischer Gleichungen gehören etwa

Beispiele 2.10.

a) $x^2 + y^2 - z^2 = 0$;

b) $x^2 - y^2 - z^2 = 0$;

c) $xz - y^2 = 0$;

d) $2x^2 - 7y^2 - z^2 = 0$;

e) $x^2 - 29y^2 - z^2 = 0$;

f) $x^2 - 2xy + y^2 + 2z^2 - xz - yz = 0$.

•

Wir wollen nun diese Klasse von Gleichungen definieren und eingehender betrachten. Die Basis der in 2.8 beschriebenen Lösungsidee – die Bestimmung der rationalen Punkte der Kurve $F(u, v, 1) = 0$ – werden wir allerdings erst im nächsten Kapitel systematisch behandeln.

Definitionen 2.11. A) Eine *homogene diophantische Quadrik* in den Unbestimmten x, y, z ist ein Polynom $Q = Q(x, y, z)$ der Form

$$Q(x, y, z) = Ax^2 + Cy^2 + Fz^2 + Bxy + Dxz + Eyz$$

mit $A, B, C, D, E, F \in \mathbb{Z}$.

B) Es gelten die obigen Bezeichnungen. Die Zahl

$$\Delta_Q := 4ACF + BDE - AE^2 - CD^2 - FB^2$$

heisst die *Diskriminante von* Q. Ist $\Delta_Q \neq 0$, so sagt man, die Quadrik Q sei *nichtausgeartet*. Ist $\Delta_Q = 0$, so heisst Q *ausgeartet*.

C) Eine *homogene quadratische diophantische Gleichung* in den Unbekannten x, y, z ist eine Gleichung der Form

$$Q(x, y, z) = 0,$$

in welcher $Q(x, y, z)$ eine homogene diophantische Quadrik ist. Ist zudem $\Delta_Q \neq 0$, so spricht man von einer *nichtausgearteten homogenen quadratischen diophantischen Gleichung*. •

Aufgaben 2.12. A) Bestimmen Sie für jede der Gleichungen aus 2.10 die 6 Koeffizienten A, B, C, D, E, F aus 2.11 A).

B) Zeigen Sie, dass alle Gleichungen aus 2.10 nichtausgeartet sind.

C) Bestimmen Sie zu jeder der diophantischen Gleichungen 2.10 a), b), c), d), f) ein (möglichst einfaches) Lösungstripel $(x, y, z) \in \mathbb{Z}^3$ mit $z = 1$.

D) Lösen Sie Aufgabe C) auch für die Gleichung 2.10 e), wobei ein Lösungstripel (x, y, z) mit $y \neq 1$ anzugeben ist. •

Sofort lässt sich ein Teil dessen, was wir in 2.8 über die Gleichung 2.10 a) gesagt haben auf beliebige homogene quadratische diophantische Gleichungen übertragen:

Bemerkung 2.13. A) Wir betrachten die homogene diophantische Quadrik (vgl. 2.11 A))

$$Q(x,y,z) = Ax^2 + Cy^2 + Fz^2 + Bxy + Dxz + Eyz$$

und interessieren uns für die nichttrivialen Lösungen der diophantischen Gleichung $Q(x,y,z) = 0$, also für die Menge

a) $$\mathbb{L}(Q) := \left\{(x_0,y_0,z_0) \in \mathbb{Z}^3 \setminus \{(0,0,0)\} \,|Q(x_0,y_0,z_0) = 0\right\}.$$

Wir definieren

b) $$\begin{cases} \mathbb{L}_x(Q) := & \{(x_0,y_0,z_0) \in \mathbb{L}(Q) | x_0 \neq 0\}; \\ \mathbb{L}_y(Q) := & \{(x_0,y_0,z_0) \in \mathbb{L}(Q) | y_0 \neq 0\}; \\ \mathbb{L}_z(Q) := & \{(x_0,y_0,z_0) \in \mathbb{L}(Q) | z_0 \neq 0\}. \end{cases}$$

Dann gilt natürlich

$$\mathbb{L}(Q) = \mathbb{L}_x(Q) \cup \mathbb{L}_y(Q) \cup \mathbb{L}_z(Q).$$

Um $\mathbb{L}(Q)$ zu bestimmen genügt es also, die drei Mengen $\mathbb{L}_x(Q), \mathbb{L}_y(Q)$ und $\mathbb{L}_z(Q)$ zu bestimmen.

B) Will man ein allgemeines Lösungsprinzip für die diophantische Gleichung $Q(x,y,z) = 0$ angeben, so kann man sich ohne Einschränkung der Allgemeinheit auf die Bestimmung der Menge $\mathbb{L}_z(Q)$ beschränken. In den folgenden Bemerkungen wollen wir dies so halten und einiges, was wir in 2.8 für die Gleichung $x^2 + y^2 - z^2 = 0$ gesagt haben auf beliebige homogene quadratische diophantische Gleichungen übertragen. Wir halten dazu die obigen Bezeichnungen fest und setzen

$$f(u,v) := Q(u,v,1),$$

sodass gilt

$$f(u,v) = Au^2 + Buv + Cv^2 + Du + Ev + F.$$

Man nennt $f = f(u,v)$ eine *Quadrik in u und v*. Nun setzen wir:

$$\mathbb{M}(f) := \{(u,v) \in \mathbb{R}^2 | f(u,v) = 0\}.$$

Im allgemeinen wird $\mathbb{M}(f)$ eine Kurve in der Ebene sein. Sofort sieht man:

$$(x_0,y_0,z_0) \in \mathbb{L}_z(Q) \Longrightarrow (u_0,v_0) := \left(\frac{x_0}{z_0}, \frac{y_0}{z_0}\right) \in \mathbb{Q}^2 \cap \mathbb{M}(f).$$

C) Die Aussage 2.8 C) a) lässt sich nun leicht auf unsere homogene quadratische Gleichung übertragen (vgl. 1.8 B) c)):

a) $\mathbb{L}_z(Q) = \{(z_0u_0, z_0v_0, z_0) | (u_0,v_0) \in \mathbb{Q}^2 \cap \mathbb{M}(f), z_0 \in \mathbb{Z}\setminus\{0\}$ so, dass $z_0u_0, z_0v_0 \in \mathbb{Z}\}$.

Insbesondere können wir sagen:

b) $$\mathbb{L}_z(Q) = \emptyset \Longleftrightarrow \mathbb{Q}^2 \cap \mathbb{M}(f) = \emptyset.$$

•

Die Aussage 2.13 C) a) bringt etwas zum Ausdruck, was wir schon aus 1.8 wissen:

- *Um die (Teil-)Lösungsmenge $\mathbb{L}_z(Q)$ der homogenen quadratischen diophantischen Gleichung $Q(x, y, z) = 0$ zu beschreiben genügt es, die Menge $\mathbb{Q}^2 \cap \mathbb{M}(f)$ der rationalen Punkte der Quadrik $f(u, v) = Q(u, v, 1)$ zu beschreiben.*

Aufgaben 2.14. A) Beweisen Sie die Aussage 2.13 C) a).

B) Skizzieren Sie $\mathbb{M}(f)$ (mit $f := f(u, v) = Q(u, v, 1)$) für

a) $Q(x, y, z) = xz - y^2$;

b) $Q(x, y, z) = x^2 - y^2 - z^2$;

c) $Q(x, y, z) = x^2 + y^2 - 7z^2$;

d) $Q(x, y, z) = -x^2 + 2y^2 - 3z^2$.

•

Zur Existenz nichttrivialer Lösungen

Wir werden später lernen, wie man mit Hilfe einer sogenannten *rationalen Parametrisierung der Quadrik* $f(u, v) = Q(u, v, 1)$ deren rationale Punkte, also die Menge $\mathbb{Q}^2 \cap \mathbb{M}(f)$ beschreibt. Gemäss dem oben Gesagten lässt sich dann auch die Menge $\mathbb{L}_z(Q)$ beschreiben. Es kann allerdings vorkommen, dass die Menge $\mathbb{L}_z(Q)$ leer ist, also dass die Menge $\mathbb{M}(f)$ keine rationalen Punkte enthält, obwohl $\mathbb{M}(f)$ eine „ganze Kurve“ ist. Wie schon im Überblick zu diesem Kapitel gesagt, übersteigt die systematische Behandlung dieses Phänomens unsere Möglichkeiten. Trotzdem wollen wir zwei Beispiele dazu anführen.

Beispiel 2.15. A) Wir betrachten die homogene quadratische diophantische Gleichung

a) $$x^2 + y^2 - 7z^2 = 0$$

und wollen zeigen, dass diese nur die triviale Lösung hat, also dass (vgl. 2.13 A) a)):

b) $$\mathbb{L}(x^2 + y^2 - 7z^2) = \emptyset.$$

Wir nehmen an, es sei $(x_0, y_0, z_0) \in \mathbb{L}(x^2+y^2-7z^2)$ und leiten daraus eine Widerspruch her. Nach weglassen gemeinsamer Faktoren können wir annehmen x_0, y_0 und z_0 hätten keinen gemeinsamen Teiler, also (vgl. 5.4)

c) $$\mathbb{P}(x_0) \cap \mathbb{P}(y_0) \cap \mathbb{P}(z_0) = \emptyset.$$

Nun können wir schreiben:

$$x_0 = 7m + r \text{ mit } m \in \mathbb{Z} \text{ und } r \in \{0, 1, \cdots, 6\};$$

$$y_0 = 7n + s \text{ mit } n \in \mathbb{Z} \text{ und } s \in \{0, 1, \cdots, 6\}.$$

Aus c) ergibt sich zusätzlich

d) $$(r, s) \neq (0, 0).$$

Einsetzen in die Gleichung a) liefert

$$\begin{aligned} 7z^2 = x^2 + y^2 &= (7m+r)^2 + (7n+s)^2 = 49m^2 + 14mr + r^2 + 49n^2 + 14ns + s^2 \\ &= 7(7m^2 + 2mr + 7n^2 + 2ns) + r^2 + s^2. \end{aligned}$$

Also können wir sagen (vgl. auch d)):

e) $$\exists r, s \in \{0, 1, \cdots, 6\} : 7 | r^2 + s^2 \neq 0.$$

Wir tabellieren die Werte von $r^2 + s^2$ für $r, s \in \{0, 1, \ldots, 6\}$:

s \ r	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	1	4	9	16	25	36
1	1	2	5	10	17	26	37
2	4	5	8	13	20	29	40
3	9	10	13	18	25	34	45
4	16	17	20	25	32	41	52
5	25	26	29	34	41	50	61
6	36	37	40	45	52	61	72

Die Tabelle zeigt, dass Aussage e) nicht gilt.

B) Insbesondere folgt aus der Aussage A) b):

$$\mathbb{L}_z(x^2 + y^2 - 7z^2) = \emptyset.$$

Gemäss Aussage 2.13 C) b) ergibt sich daraus

$$\mathbb{Q}^2 \cap \mathbb{M}(u^2 + v^2 - 7) = \emptyset.$$

Die Quadrik $\mathbb{M}(u^2 + v^2 - 7)$ enthält also keinen einzigen rationalen Punkt, obwohl $\mathbb{M}(u^2 + v^2 - 7)$ „sehr viele“ Punkte enthält:
Für jedes $u \in [-\sqrt{7}, \sqrt{7}]$ gilt $(u, \pm\sqrt{7 - u^2}) \in \mathbb{M}(u^2 + v^2 - 7)$ (vgl. auch 2.14 B) c)). •

Wir betrachten ein weiteres Beispiel.

Beispiel 2.16. A) Wir wollen zeigen, dass

a) $$\mathbb{L}(-x^2 + 2y^2 - 3z^2) = \emptyset.$$

Wir nehmen im Gegenteil an, es gäbe ein Tripel $(x_0, y_0, z_0) \in \mathbb{L}(-x^2+2y^2-3z^2)$. Wieder können wir annehmen, es sei

$$\mathbb{P}(x_0) \cap \mathbb{P}(y_0) \cap \mathbb{P}(z_0) = \emptyset$$

und schreiben

$$x_0 = 3m + r \text{ mit } m \in \mathbb{Z} \text{ und } r \in \{0, 1, 2\};$$
$$y_0 = 3n + s \text{ mit } n \in \mathbb{Z} \text{ und } s \in \{0, 1, 2\};$$

b) $$(r, s) \neq (0, 0).$$

Es folgt

$$\begin{aligned} 3z_0^2 &= -x_0^2 + 2y_0^2 = 2(3n + s)^2 - (3m + r)^2 = 18n^2 + 12ns + 2s^2 - 9m^2 - 6mr - r^2 \\ &= 3(6n^2 + 4ns - 3m^2 - 2mr) + 2s^2 - r^2, \end{aligned}$$

also

c) $$3|2s^2 - r^2.$$

Wir tabellieren die Werte von $2s^2 - r^2$ für $r, s \in \{0, 1, 2\}$ und sehen, dass die Aussagen b) und c) nicht gleichzeitig gelten können:

r \ s	**0**	**1**	**2**
0	0	2	8
1	-1	1	7
2	-4	-2	4

B) Aus der Aussage A) a) folgt wieder

$$\mathbb{L}_z(-x^2 + 2y^2 - 3z^2) = \emptyset$$

und damit

$$\mathbb{Q}^2 \cap \mathbb{M}(-u^2 + 2v^2 - 3) = \emptyset.$$

Die Quadrik $\mathbb{M}(-u^2 + 2v^2 - 3)$ enthält also wieder keinen rationalen Punkt, obwohl $\left(u, \pm\sqrt{\frac{3+u^2}{2}}\right) \in \mathbb{M}(-u^2 + 2v^2 - 3)$ für jede Zahl $u \in \mathbb{R}$ (vgl. Aufgabe 2.14 B) d)). •

Aufgaben 2.17. A) Bestimmen Sie die Mengen

a) $$\mathbb{L}(x^2 + y^2 - 3z^2);$$

b) $$\mathbb{M}(u^2 + v^2 - 3).$$

B) Bestimmen Sie alle Zahlen $c \in \{1, 2, \cdots, 10\}$ mit

$$\mathbb{L}(x^2 + y^2 - cz^2) = \emptyset.$$

C) Sei $(a_n)_{n\in\mathbb{N}}$ eine Folge positiver rationaler Zahlen mit $\lim_{n\to\infty} a_n = \sqrt{7}$. Sei weiter $f_n = f_n(u, v) = u^2 + v^2 - \frac{a_n^2}{7}$. Zeigen Sie, dass $\mathbb{Q}^2 \cap \mathbb{M}(f_n) = \emptyset$ und beschreiben Sie die Folge der Mengen $\mathbb{M}(f_n)$ geometrisch.

D) Lösen Sie Aufgabe C) mit $f_n = f_n(u, v) = \frac{a_n^2}{7}\, u^2 + \frac{7}{a_n^2}\, v^2 - 1$. •

Kapitel 3

Rationale Punkte auf Quadriken

Überblick

In diesem Kapitel soll die rationale Parametrisierung des Einheitskreises, welche wir in Kapitel 2 erfolgreich für die Bestimmung der pythagoräischen Tripel eingesetzt haben, auf beliebige nichtausgeartete ebene Quadriken übertragen werden. Wir werden also die rationale Parametrisierung nichtausgearteter ebener Quadriken behandlen. Dieses an sich rein geometrische Prinzip ist von grösster Bedeutung für die in Kapitel 2 behandelten nichtausgearteten homogenen quadratischen diophantischen Gleichungen. Es liefert nämlich eine Methode um aus einer einzigen nichttrivialen Lösung einer solchen diophantischen Gleichung alle andern nichttrivialen Lösungen zu finden. Mit dieser Illustration der intensiven Wechselwirkung zwischen Arithmetik und Geometrie der Kegelschnitte schliesst sich der thematische Hauptkreis Kreis unseres Kurses weitgehend: Unbehandelt muss nur die Frage bleiben, wie man denn überhaupt zu einer nichttrivialen Lösung kommt.

Dieses Kapitel kann auch als eine erste Einführung in die ebene algebraische Geometrie verstanden werden. In der Sprache der algebraischen Geometrie ausgedrückt besteht dieses Kapitel im Wesentlichen aus einem konstruktiven Beweis der Tatsache, dass nichtausgeartete ebene Quadriken – oder eben die Kegelschnitte – rationale Kurven sind.

Es werden folgende Themen behandelt:

- *Eine Vorbetrachtung*,
- *Ebene Quadriken*,
- *Partielle Ableitungen und Diskriminanten*,
- *Quadriken und Geraden*,
- *Geometrische Bedeutung der Tangenten und der kritischen Geraden*,

- *Rationale Parametrisierung der Quadriken*,

Haben wir beim Kapitel 1 von einer „Schnupperlehre in Diophantik“gesprochen, so könnten wir bei diesem Kapitel von einer „Schnupperlehre in algebraischer Geometrie“reden. Allerdings ist der Stil nun ganz anders als in Kapitel 1. Es wird uns hier um eine systematische und strenge Behandlung eines zentralen Themas gehen und nicht mehr um ein Hüpfen von Einzelfall zu Einzelfall.

Eine Vorbetrachtung

In diesem Abschnitt wollen wir den Inhalt des vorliegenden Kapitels zusammenfassend darstellen.

Bemerkung 3.1. Sei

$$Q(x, y, z) = Ax^2 + Cy^2 + Fz^2 + Bxy + Dxz + Eyz$$

eine homogene diophantische Quadrik (vgl. 2.11 A)). Wie in 2.13 A) a)) stehe $\mathbb{L}(Q)$ wieder für die Menge der nichttrivialen Lösungen der diophantischen Gleichung $Q(x, y, z) = 0$. Wie in 2.13 A) b) schreiben wir wieder $\mathbb{L}_z(Q)$ für die Menge aller Tripel $(x_0, y_0, z_0) \in \mathbb{L}(Q)$ mit $z_0 \neq 0$. Wir sind interessiert an einem Verfahren, das es erlaubt, aus einer einzigen Lösung $(x_0, y_0, z_0) \in \mathbb{L}(Q)$ alle andern Lösungen zu gewinnen.

Wie wir schon in 2.13 B) bemerkt haben, genügt es, ein Verfahren anzugeben, mit dem sich aus einer einzigen Lösung $(x_0, y_0, z_0) \in \mathbb{L}_z(Q)$ alle andern Tripel in $\mathbb{L}_z(Q)$ gewinnen lassen.

Das Verfahren, das wir beschreiben wollen, beruht auf einer geometrischen Idee und macht sich zu Nutzen, was wir bereits in 2.13 B), C) festgestellt haben:

Die Menge $\mathbb{L}_z(Q)$ lässt sich aus der Menge $\mathbb{Q}^2 \cap \mathbb{M}(f)$ der rationalen Punkte der Quadrik

$$f = f(u, v) = Q(u, v, 1) = Au^2 + Buv + Cv^2 + Du + Ev + F$$

gewinnen.

Es genügt also, ein Verfahren anzugeben, welches erlaubt, aus einem Punkt $(u_0, v_0) \in \mathbb{Q}^2 \cap \mathbb{M}(f)$ alle Punkte von $\mathbb{Q}^2 \cap \mathbb{M}(f)$ zu gewinnen. •

Wir wollen das oben erwähnte Verfahren im folgenden kurz skizzieren. Es handelt sich um die *rationale Parametrisierung von Quadriken.*

Konstruktion 3.2. A) Wir betrachten wieder die homogene diophantische Quadrik

$$Q(x,y,z) = Ax^2 + Cy^2 + Fz^2 + Bxy + Dxz + Eyz.$$

Zusätzlich wollen wir annehmen, dass $Q = Q(x,y,z)$ nichtausgeartet ist, also dass (vgl. 2.11 B))

$$\Delta_Q := 4ACF + BDE - AE^2 - CD^2 - FB^2 \neq 0.$$

Wir betrachten die zugehörige *ebene Quadrik*

$$f = f(u,v) := Q(u,v,1) = Au^2 + Buv + Cv^2 + Du + Ev + F$$

und deren Nullstellenmenge

$$\mathbb{M}(f) = \{(u,v) \in \mathbb{R}^2 \,\big|\, f(u,v) = 0\}.$$

Wir wollen annehmen, es sei

$$S = (u_0, v_0) \in \mathbb{Q}^2 \cap \mathbb{M}(f).$$

Nun soll also ein Verfahren angegeben werden, welches erlaubt, aus S alle Punkte von $\mathbb{Q}^2 \cap \mathbb{M}(f)$ zu gewinnen.

B) Als erstes legen wir eine Tangente an die Kurve $\mathbb{M}(f)$ im Punkt $S = (u_0, v_0)$ (vgl. 3.13 B)). Dann legen wir eine Hilfsgerade h, welche parallel ist zur gelegten Tangente. Diese Hilfsgerade besitzt dann eine Parameterdarstellung der Form (vgl.3.18 A) b))

$$h : t \mapsto P_t := (u_0 + b + at, v_0 - a + bt);\ (t \in \mathbb{R}),$$

wobei a und b geeignete rationale Zahlen sind, die nicht beide verschwinden. Zu jedem Parameterwert $t \in \mathbb{R}$ legen wir nun die Gerade g_t durch die Punkte P_t und S. Dann schneiden wir die Kurve $\mathbb{M}(f)$ mit der Geraden g_t.

Wir werden später zeigen, dass folgendes gilt: Vermeidet t gewisse „kritische Werte“, so haben $\mathbb{M}(f)$ und g_t nebst S noch genau einen weiteren Schnittpunkt, den wir mit $S_t = (u(t), v(t))$ bezeichnen (vgl. 3.18 C)).

Es treten höchstens zwei der genannten kritischen Werte auf. Für diese kritischen Werte von t ist S der einzige Schnittpunkt von $\mathbb{M}(f)$ mit g_t (vgl. 3.18 C)).

Schreiben wir $\mathcal{C}$ für die Menge der (höchstens zwei) kritischen Parameterwerte, so erhalten wir eine bijektive Abbildung (vgl. 3.20)

$$\varepsilon_S = \varepsilon : \mathbb{R}\backslash\mathcal{C} \xrightarrow{\approx} \mathbb{M}\backslash\{S\};\ t \mapsto \varepsilon(t) := (u(t), v(t)).$$

Dabei gilt, wie wir später beweisen werden (vgl. 3.21):

$$t \in \mathbb{Q} \Longleftrightarrow \varepsilon(t) \in \mathbb{Q}^2;\ (t \in \mathbb{R}\backslash\mathcal{C}).$$

Insbesondere gilt also (vgl. 3.22 b))

$$\mathbb{Q}^2 \cap \mathbb{M}(f) = (u_0, v_0) \cup \{\varepsilon(t) = (u(t), v(t)) \,|\, t \in \mathbb{Q}\backslash\mathcal{C}\}.$$

Damit sind alle Punkte von $\mathbb{Q}^2 \cap \mathbb{M}(f)$ vermöge $\varepsilon = \varepsilon_S = \varepsilon_{(u_0,v_0)}$ parametrisiert, und das gewünschte Ziel ist erreicht.

C) Im folgenden ist die soeben beschriebene Methode der rationalen Parametrisierung einer Quadrik f anschaulich illustriert. Wir haben dabei an den Fall gedacht, wo $\mathbb{M}(f)$ eine Parabel ist (vgl. 3.6 C)). In diesem Fall tritt ein kritischer Wert auf (vgl. 3.16 D) (δ')).

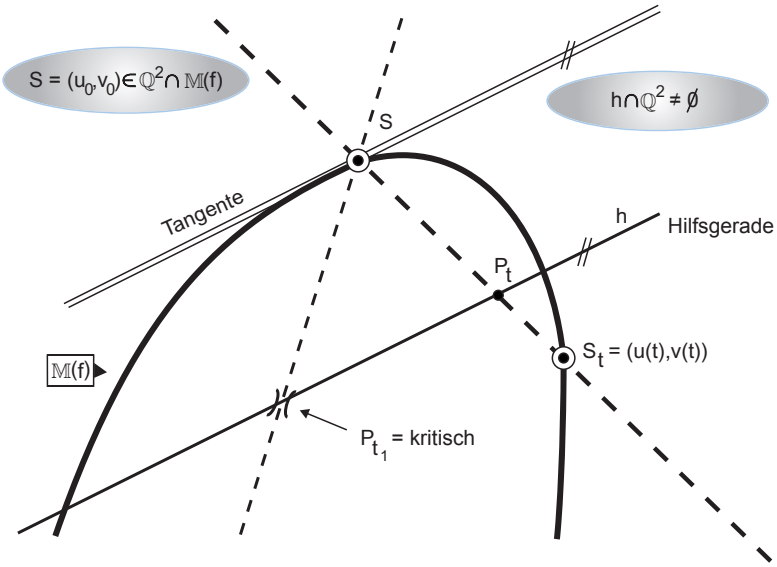


Abbildung 3.1: Rationale Parametrisierung einer Quadrik

•

Bemerkung 3.3. A) Im Spezialfall $A = C = 1, B = D = E = 0$ und $F = 1$ gilt $f(u, v) = u^2 + v^2 - 1$. In diesem Fall ist $\mathbb{M} = \mathbb{M}(f)$ gerade der Einheitskreis. Wählt man $S = (u_0, v_0) = (0, 1)$, ist h die u-Achse und setzt man $a = 1$ und $b = 0$, so liefert das in 3.2 beschriebene Verfahren gerade die in 2.3 vorgenommene rationale Parametrisierung des Einheitskreises.

B) Man könnte im allgemeinen Fall die tangentenparallele Hilfsgerade h ersetzen durch irgendeine Gerade h', welche den Punkt $S = (u_0, v_0)$ vermeidet. Die arithmetische Handhabung der Parametrisierung könnte sich damit sogar vereinfachen. Andererseits wäre dann ein „Schönheitsfehler“in Kauf zu nehmen: Es tritt ein zusätzlicher kritischer Parameterwert auf! Deswegen könnte bei der Parametrisierung ein Punkt in $\mathbb{Q}^2 \cap \mathbb{M}(f)$ „verloren gehen“d.h. nicht erfasst werden. Aus diesem Grund werden wir nur den Fall weiterverfolgen, in dem die Hilfsgerade h parallel zur Tangente zu f in $S = (u_0, v_0)$ ist.•

Aufgaben 3.4. A) Wählen Sie $A = \frac{1}{4}, C = 1, F = -1$ und $B = D = E = 0$. Wählen Sie $S = (0, 1)$ und wählen Sie die Hilfsgerade h so, dass $P_0 := (0, 0) \in h$. Berechnen Sie die beiden Funktionen $u(t)$ und $v(t)$ aus 3.2 B) und bestimmen Sie die Menge $\mathcal{C} \subseteq \mathbb{R}$ aller kritischen Werte. Skizzieren Sie die Situation im Sinne der Abbildung 3.1.

B) Lösen Sie Aufgabe A) für $A = B = E = F = 0, C = 1$ und $D = -1$ mit $S = (0, 0)$, wobei $P_0 := (-1, 0) \in h$.

C) Lösen Sie dieselbe Aufgabe, aber mit $A = 1, C = F = -1, B = D = E = 0, S = (1, 0)$ und $P_0 = (0, 0) \in h$.

D) Wählen Sie in jedem der Beispiele aus A)–C) eine Hilfsgerade $h' \neq h$ durch den jeweils vorgeschlagenen Punkt P_0. Machen Sie damit das in 3.3 B) Gesagte anschaulich an einer Skizze klar. •

Ebene Quadriken

Wir wollen uns nun daran machen, die im vorangehenden Abschnitt beschriebene Konstruktion wirklich durchzuführen und streng zu begründen. Wir beginnen mit dem „Grundmaterial“unserer Konstruktion: Den *ebenen Quadriken*, d.h. den Quadriken in zwei Unbestimmten.

Definition 3.5. A) Eine *Quadrik in den Unbestimmten* u und v ist ein Polynom vom Grad 2 in zwei Unbestimmten u und v mit reellen Koeffizienten, also ein Polynom der Form

$$f(u, v) = Au^2 + Buv + Cv^2 + Du + Ev + F$$

mit

$$A, B, C, D, E, F \in \mathbb{R}.$$

B) Die Zahl

$$\Delta_f := 4ACF + BDE - AE^2 - CD^2 - FB^2$$

heisst die *Diskriminante* der Quadrik $f = f(u, v)$. Man nennt die Quadrik f *ausgeartet*, wenn $\Delta_f = 0$. Man nennt f *nichtausgeartet*, wenn $\Delta_f \neq 0$, also wenn

$$4ACF + BDE - AE^2 - CD^2 - FB^2 \neq 0.$$

C) Ist $f = f(u, v)$ eine Quadrik, so schreiben wir $\mathbb{M}$ oder $\mathbb{M}(f)$ für die Menge aller reellen Lösungspaare (u, v) der Gleichung $f(u, v) = 0$. Also

$$\mathbb{M} = \mathbb{M}(f) := \{(u, v) \in \mathbb{R}^2 \,\big|\, f(u, v) = 0\}.$$

D) Die Quadrik

$$f(u, v) = Ax^2 + Bxy + Cy^2 + Dx + Ey + F$$

heisst *rational*, wenn ihre Koeffizienten rationale Zahlen sind, d.h. wenn

$$A, B, C, D, E, F \in \mathbb{Q}.$$

•

Wir wollen nun als Beispiele einige besonders einfache aber wichtige Spezialfälle nichtausgearteter rationaler Quadriken betrachten und geometrisch einordnen.

Spezialfälle und Beispiele 3.6. A) Wir betrachten den Fall der rationalen Quadrik $f(u, v) = u^2 + v^2 - 1$, d.h. den Fall

$$A = C = 1, F = -1, B = D = E = 0.$$

Hier ist $\mathbb{M} = \mathbb{M}(f)$ der Einheitskreis. Die rationalen Punkte auf dieser Menge $\mathbb{M}$ haben wir bereits eingehend studiert.

B) Wir betrachten die rationale Quadrik

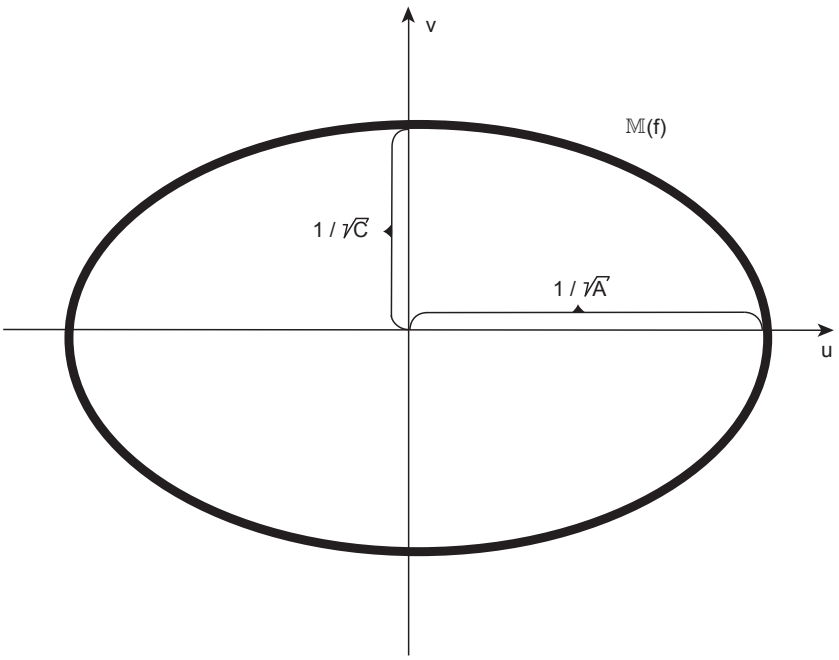


Abbildung 3.2: Ellipse

$$f(u, v) = Au^2 + Cv^2 - 1; \quad (0 < A \leq C),$$

d.h. den Fall

$$0 < A \leq C, F = -1, B = D = E = 0.$$

Hier ist $\mathbb{M} = \mathbb{M}(f)$ eine *Ellipse* mit *grosser Halbachse* $1/\sqrt{A}$ und *kleiner Halbachse* $1/\sqrt{C}$.

C) Wir betrachten die rationale Quadrik

$$f(u,v) = Cv^2 - u - 1; \quad (C > 0),$$

d.h. den Fall

$$A = B = E = 0, C > 0, D = F = -1.$$

Es handelt sich bei $\mathbb{M} = \mathbb{M}(f)$ um eine *Parabel* durch die 3 Punkte $(-1,0), (0, \pm\sqrt{1/C})$.

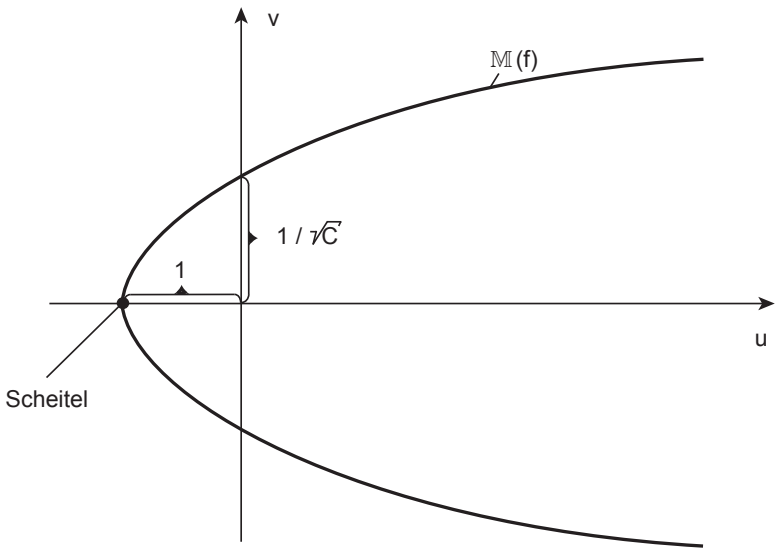


Abbildung 3.3: Parabel

D) Schliesslich betrachten wir noch die rationale Quadrik

$$f(u,v) = Au^2 + Cv^2 - 1; \quad (A < 0 < C),$$

also den Fall

$$B = D = E = 0, \ A < 0 < C, F = -1.$$

Es handelt sich bei $\mathbb{M} = \mathbb{M}(f)$ nun um eine *Hyperbel*. Die Asymptoten der Hyperbel $\mathbb{M}$ sind die beiden Geraden mit den Gleichungen

$$v = \pm\sqrt{-\frac{A}{C}}\, u.$$

Die Scheitelpunkte der Hyperbel sind $(0, \pm\sqrt{\frac{1}{C}})$.

•

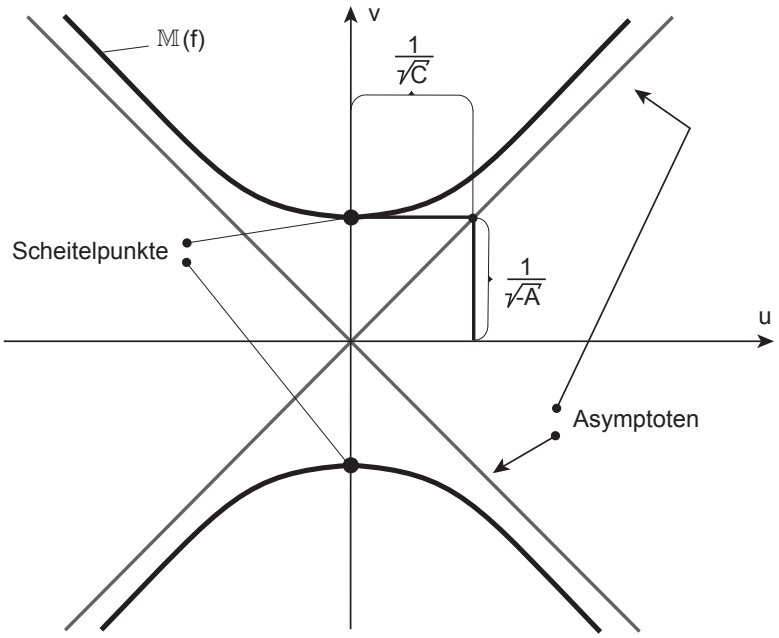


Abbildung 3.4: Hyperbel

Aufgaben 3.7. A) Zeigen Sie, dass die vorangehenden Beispiele aus 3.6 A)–D) nichtausgeartete (rationale) Quadriken sind.

B) Sei $f(u,v) = Au^2+Buv+Cv^2+Du+Ev+F$ eine nichtausgeartete rationale Quadrik. Zeigen Sie, dass folgende Polynome nichtausgeartete rationale Quadriken sind:

a) $f(v,u)$;

b) $\alpha f(u,v), (\alpha \in \mathbb{Q}\backslash\{0\})$;

c) $f(\alpha u,v), (\alpha \in \mathbb{Q}\backslash\{0\})$;

d) $f(u+\gamma,v), (\gamma \in \mathbb{Q})$;

e) $f(u+\gamma v,v), (\gamma \in \mathbb{Q})$.

C) Ellipsen, Parabeln und Hyperbeln sind sogenannte *Kegelschnitte*. Können Sie diesen Begriff erklären?

D) Zeigen Sie, dass die folgenden Quadriken f nichtausgeartet sind und skizzieren Sie jeweils $\mathbb{M}(f)$:

a) $f(v,u) = u^2+v^2+1$;

b) $\alpha f(u,v), (\alpha \in \mathbb{Q}\backslash\{0\})$;

c) $f(u,v) = u^2 + v^2 - 2u$;

d) $f(u+\gamma, v), (\gamma \in \mathbb{Q})$;

e) $f(u,v) = u^2 + uv + v^2 - 1$.

E) Sei f wie in B). Zeigen Sie, dass f durch wiederholtes Anwenden der Transformationen a)–e) aus B) übergeführt werden kann in eine der 4 Quadriken $u^2 + v^2 + 1, u^2 + v^2 - 1, -u^2 + v^2 - 1, v^2 - u - 1$. •

Partielle Ableitungen und Diskriminanten

In diesem Unterabschnitt beweisen wir eine Formel für die Diskriminante einer Quadrik – die bereits in Definition 3.5 B) eingefhrt wurde – und wenden diese Formel dann an. Wir benötigen dabei den Begriff der partiellen Ableitung. Wir fixieren eine Quadrik

$$f = f(u,v) = Au^2 + Buv + Cv^2 + Du + Ev + F$$

und rufen in Erinnerung, dass die Diskriminante von f gegeben ist durch

$$\Delta_f := 4ACF + BDE - AE^2 - CD^2 - FB^2.$$

Definition und Bemerkung 3.8. A) Die *partielle Ableitung*

$$\frac{\partial f}{\partial u} = \frac{\partial f}{\partial u}(u,v)$$

der Funktion $f = f(u,v)$ *bezüglich* (oder *nach*) u ist die Ableitung der Funktion $f(u,v)$ nach der Variablen u, wenn v als Konstante betrachtet wird.

Entsprechend ist auch die *partielle Ableitung*

$$\frac{\partial f}{\partial v} = \frac{\partial f}{\partial v}(u,v)$$

der Funktion $f = f(u,v)$ *bezüglich* (oder *nach*) v definiert: als die Ableitung der Funtkon $f(u,v)$ nach der Variablen v bei konstantem u.

B) Der Graph

$$\{(u,v,f(u,v)) \,|\, u,v \in \mathbb{R}\} \subseteq \mathbb{R}^3$$

der Funktion $f = f(u,v)$ entspricht einer Fläche im Raum. Sind $u_0, v_0 \in \mathbb{R}$, so folgt aus der wohlbekannten Interpretation der gewöhnlichen Ableitung als Steigung (der Tangente) des Graphen:

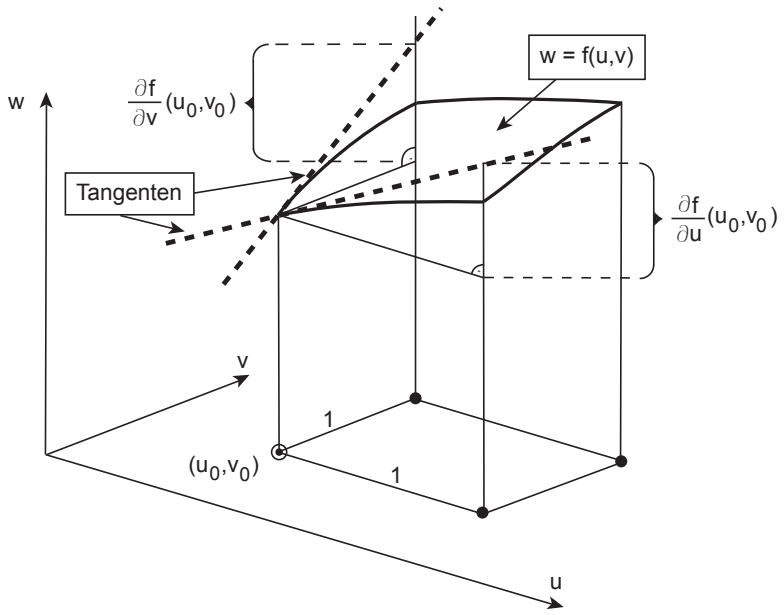


Abbildung 3.5: Partielle Ableitungen

$\frac{\partial f}{\partial u}(u_0, v_0)$ *ist die Steigung des Graphen von* f *in Richtung* u *an der Stelle* (u_0, v_0)*,*

$\frac{\partial f}{\partial v}(u_0, v_0)$ *ist die Steigung des Graphen von* f *in Richtung* v *an der Stelle* (u_0, v_0)*.*

C) Für unsere Quadrik $f = f(u, v)$ erhält man sofort:

a) $\frac{\partial f}{\partial u}(u_0, v_0) = 2Au_0 + Bv_0 + D$;

b) $\frac{\partial f}{\partial v}(u_0, v_0) = 2Cv_0 + Bu_0 + E$.

Satz 3.9. *(Diskriminantenformel) Sind* $u_0, v_0 \in \mathbb{R}$ *mit* $f(u_0, v_0) = 0$*, so gilt*

$$-\Delta_f = A\left(\frac{\partial f}{\partial v}(u_0, v_0)\right)^2 - B\frac{\partial f}{\partial u}(u_0, v_0)\frac{\partial f}{\partial v}(u_0, v_0) + C\left(\frac{\partial f}{\partial u}(u_0, v_0)\right)^2.$$

Beweis: 3.8 C) a), b) ergibt für die rechte Seite der behaupteten Gleichung den Term

$$A(2Cv_0 + Bu_0 + E)^2 - B(2Au_0 + Bv_0 + D)(2Cv_0 + Bu_0 + E) + C(2Au_0 + Bv_0 + D)^2.$$

Durch Ausmultiplizieren der einzelnen Summanden erhält man somit für die rechte Seite unserer Gleichung die Summe

$$\begin{aligned}
&\underline{4AC^2v_0^2} + \underline{AB^2u_0^2} + AE^2 + \underline{4ABCu_0v_0} + \underline{2ABEu_0} + \underline{4ACEv_0} \\
&- \underline{4ABCu_0v_0} - \underline{2AB^2u_0^2} - \underline{2ABEu_0} - \underline{2B^2Cv_0^2} \\
&- \underline{B^3u_0v_0} - \underline{B^2Ev_0} - \underline{2BCDv_0} - \underline{B^2Du_0} - BDE \\
&+ \underline{4A^2Cu_0^2} + \underline{B^2Cv_0^2} + CD^2 + \underline{4ABCu_0v_0} + \underline{4ACDu_0} + \underline{2BCDv_0}.
\end{aligned}$$

Die mit $\underline{\bullet}$ unterstrichenen Summanden ergeben zusammen

$$4AC(Au_0^2 + Bu_0v_0 + Cv_0^2 + Du_0 + Ev_0) = 4AC(f(u_0, v_0) - F) = -4ACF.$$

Die mit $\underset{\sim}{\bullet}$ unterstrichenen Summanden ergeben zusammen

$$-B^2(Au_0^2 + Bu_0v_0 + Cv_0^2 + Du_0 + Ev_0) = -B^2(f(u_0, v_0) - F) = B^2F.$$

Die mit $\underset{\approx}{\bullet}$ unterstrichenen Summanden ergeben zusammen 0. Die ganze Summe hat also den Wert

$$-4ACF + B^2F + AE^2 - BDE + CD^2 = -\Delta_f.$$

■

Korollar 3.10. *Sei $f = f(u, v)$ nichtausgeartet und seien $u_0, v_0 \in \mathbb{R}$ mit $f(u_0, v_0) = 0$. Dann gilt:*

a) $\frac{\partial f}{\partial u}(u_0, v_0) \neq 0$ *oder* $\frac{\partial f}{\partial v}(u_0, v_0) \neq 0$*;*

b) Sind $\alpha, \beta \in \mathbb{R}$ mit

$$A\alpha^2 + B\alpha\beta + C\beta^2 = \frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta = 0,$$

so folgt $\alpha = \beta = 0$.

Beweis: „a)“: Klar aus 3.9 wegen $\Delta_f \neq 0$.
„b)“: Wegen $\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta = 0$ folgt $\alpha\frac{\partial f}{\partial u}(u_0, v_0) = -\beta\frac{\partial f}{\partial v}(u_0, v_0)$. Daraus ergeben sich die Gleichungen

$$\begin{aligned}
\alpha^2\left(\frac{\partial f}{\partial u}(u_0, v_0)\right)^2 &= \beta^2\left(\frac{\partial f}{\partial v}(u_0, v_0)\right)^2, \\
\alpha^2\frac{\partial f}{\partial u}(u_0, v_0)\frac{\partial f}{\partial v}(u_0, v_0) &= -\alpha\beta\left(\frac{\partial f}{\partial v}(u_0, v_0)\right)^2, \\
\beta^2\frac{\partial f}{\partial u}(u_0, v_0)\frac{\partial f}{\partial v}(u_0, v_0) &= -\alpha\beta\left(\frac{\partial f}{\partial u}(u_0, v_0)\right)^2.
\end{aligned}$$

Nun folgt mit 3.9

$$
\begin{aligned}
&-(\alpha^2+\beta^2)\Delta_f = (\alpha^2+\beta^2)A\left(\frac{\partial f}{\partial v}(u_0,v_0)\right)^2\\
&-(\alpha^2+\beta^2)B\frac{\partial f}{\partial u}(u_0,v_0)\frac{\partial f}{\partial v}(u_0,v_0)\\
&+(\alpha^2+\beta^2)C\left(\frac{\partial f}{\partial u}(u_0,v_0)\right)^2 =\\
&A\alpha^2\left(\left(\frac{\partial f}{\partial v}(u_0,v_0)\right)^2+\left(\frac{\partial f}{\partial u}(u_0,v_0)\right)^2\right)\\
&+B\alpha\beta\left(\left(\frac{\partial f}{\partial v}(u_0,v_0)\right)^2+\left(\frac{\partial f}{\partial u}(u_0,v_0)\right)^2\right)\\
&+C\beta^2\left(\left(\frac{\partial f}{\partial v}(u_0,v_0)\right)^2+\left(\frac{\partial f}{\partial u}(u_0,v_0)\right)^2\right) =\\
&(A\alpha^2+B\alpha\beta+C\beta^2)\left(\left(\frac{\partial f}{\partial v}(u_0,v_0)\right)^2+\left(\frac{\partial f}{\partial u}(u_0,v_0)\right)^2\right)=0.
\end{aligned}
$$

Wegen $\Delta_f \neq 0$ folgt $\alpha^2+\beta^2=0$. ■

Quadriken und Geraden

Jetzt wollen wir uns den Beziehungen zwischen Quadriken und Geraden zuwenden. Wieder fixieren wir ein Quadrik

$$f = f(u,v) = Au^2+Buv+Cv^2+Du+Ev+F.$$

Notation und Festsetzung 3.11. A) Wir betrachten einen Punkt $S=(u_0,v_0)\in \mathbb{M}(f)=\mathbb{M}$, d.h. einen Punkt mit $f(u_0,v_0)=0$. Zudem wählen wir eine Gerade g, welche durch den Punkt $S=(u_0,v_0)$ läuft. Wir werden uns später speziell für die Schnittpunkte von $\mathbb{M}(f)$ und g interessieren, d.h. für die Menge $\mathbb{M}(f)\cap g$.
Die Gerade g sei durch die folgende Parameterdarstellung beschrieben

a) $\quad g: s\mapsto (u_0+\alpha s, v_0+\beta s)$, wobei $(\alpha,\beta)\in\mathbb{R}^2\backslash\{(0,0)\}$.

B) Die *Richtung* der Geraden g ist bestimmt durch den „Winkel φ zwischen der positiven u-Achse und g“genauer durch den Winkel (im Bogenmass)

a)
$$\varphi := \begin{cases} \arctan\left(\frac{\beta}{\alpha}\right), & \text{falls } \alpha\neq 0;\\ \frac{\pi}{2}, & \text{falls } \alpha = 0.\end{cases}$$

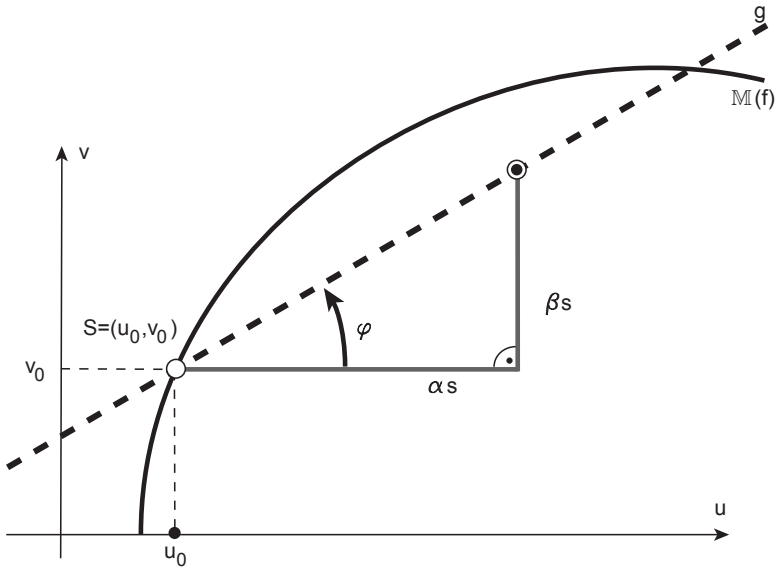


Abbildung 3.6: Quadrik und Gerade

Die *Distanz* des Punktes $\odot = (u_0 + \alpha s, v_0 + \beta s)$ vom Punkt $S = (u_0, v_0)$ ist natürlich gerade gegeben durch

b) $$\text{dist}\,((u_0, v_0), (u_0 + \alpha s, v_0 + \beta s)) = |s|\sqrt{\alpha^2 + \beta^2}.$$

•

Für die Schnittpunkte der Quadrik $\mathbb{M} = \mathbb{M}(f)$ und der Geraden g gilt nun der nachfolgende Satz, auf dem alle späteren Ausführungen beruhen werden.

Satz 3.12. *Sei $f = f(u, v)$ nichtausgeartet und sei $S = (u_0, v_0) \in \mathbb{M}(f) = \mathbb{M}$. Sei g definiert wie in 3.11. Dann gilt:*

a) Gilt $A\alpha^2 + B\alpha\beta + C\beta^2 = 0$ oder

$$\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta = 0,$$

so ist S der einzige Schnittpunkt von $\mathbb{M}$ und g.

b) Gelten $A\alpha^2 + B\alpha\beta + C\beta^2 \neq 0$ und

$$\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta \neq 0,$$

so haben $\mathbb{M}$ und g nebst S noch genau einen weiteren Schnittpunkt. Dieser ist gegeben durch $S_g = (u_0 - s_0\alpha, v_0 - s_0\beta)$, wobei

$$s_0 = \frac{\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta}{A\alpha^2 + B\alpha\beta + C\beta^2}.$$

Beweis: Der Punkt $\odot = (u_0 + s\alpha, v_0 + s\beta)$ ist genau dann ein von S verschiedener Schnittpunkt von $\mathbb{M}$ und g, wenn die folgenden beiden Aussagen gelten:

(α) $\quad f(u_0 + \alpha s, v_0 + \beta s) = 0;$

(α') $\quad s \neq 0.$

Es gilt

$$\begin{aligned}
&f(u_0 + \alpha s, v_0 + \beta s)\\
&= A(u_0 + \alpha s)^2 + B(u_0 + \alpha s)(v_0 + \beta s) + C(v_0 + \beta s)^2\\
&+ D(u_0 + \alpha s) + E(v_0 + \beta s) + F\\
&\underline{Au_0^2} + 2Au_0\alpha s + A\alpha^2 s^2 + \underline{Bu_0v_0} + u_0\beta s\\
&+ Bv_0\alpha s + B\alpha\beta s^2 + \underline{Cv_0^2} + 2Cv_0\beta s + C\beta^2 s^2\\
&+ \underline{Du_0} + D\alpha s + \underline{Ev_0} + E\beta s + \underline{F}.
\end{aligned}$$

Die unterstrichenen Terme ergeben zusammen $f(u_0, v_0) = 0$ und können deshalb weggelassen werden. Wir fassen $f(u_0 + \alpha s, v_0 + \beta s)$ als Polynom von einem Grad kleiner oder gleich 2 in s auf und ordnen entsprechend nach Potenzen von s:

$$\begin{aligned}
&f(u_0 + \alpha s, v_0 + \beta s) =\\
&(2Au_0\alpha + Bu_0\beta + Bv_0\alpha + 2Cv_0\beta + D\alpha + E\beta) + s\\
&(A\alpha^2 + B\alpha\beta + C\beta^2)s^2.
\end{aligned}$$

So erhalten wir

$$\begin{aligned}
&f(u_0 + \alpha s, v_0 + \beta s) =\\
&((2Au_0 + Bv_0 + D)\alpha + (2Cv_0 + Bu_0 + E)\beta)\, s +\\
&(A\alpha^2 + B\alpha\beta + C\beta^2)s^2.
\end{aligned}$$

Beachten wir die Formeln 3.8 C) a), b), so ergibt sich schliesslich

$$\begin{aligned}
&f(u_0 + \alpha s, v_0 + \beta s)\\
&= \left(\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta\right) s + (A\alpha^2 + B\alpha\beta + C\beta^2)s^2.
\end{aligned}$$

Die Gleichung (α) ist also äquivalent zur Gleichung

$$s\left(\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta + (A\alpha^2 + B\alpha\beta + C\beta^2)s\right) = 0.$$

Die Aussagen (α) und (α') sind also genau dann beide erfüllt, wenn die folgenden Aussagen gelten:

(β) $\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta + (A\alpha^2 + B\alpha\beta + C\beta^2)s = 0$;

(β') $s \neq 0$.

Ist $\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta = 0$, so ist $A\alpha^2 + B\alpha\beta + C\beta^2 \neq 0$ (s. 3.10 b), 3.11 A) a)). Dann können aber (β) und (β') nicht gleichzeitig gelten. Ist $A\alpha^2 + B\alpha\beta + C\beta^2 = 0$, so ist $\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta \neq 0$ (s. 3.10 b), 3.11 A) a)). Dann kann aber (β) nicht gelten. Ist also eine der beiden Grössen $A\alpha^2 + B\alpha\beta + C\beta^2$ oder $\frac{\partial f}{\partial u}(x_0, y_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta$ gleich 0, so können die Aussagen (α) und (α') nicht gleichzeitig gelten. In diesem Fall muss also S der einzige Schnittpunkt von g und $\mathbb{M}$ sein. Dies beweist die Behauptung a).

Sind $A\alpha^2 + B\alpha\beta + C\beta^2$ und $\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta$ beide verschieden von 0, so sind die beiden Aussagen (β), (β') (und damit auch die beiden Aussagen (α), (α')) genau dann erfüllt, wenn

$$s = -\frac{\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta}{A\alpha^2 + B\alpha\beta + C\beta^2}.$$

Dies beweist die Aussage b). ■

Definition und Bemerkung 3.13. A) Es gelten die Bezeichnungen von 3.11. Ist $A\alpha^2 + B\alpha\beta + C\beta^2 = 0$, so sagen wir, g sei eine (bezüglich f) *kritische Gerade durch* S. Die Bedingung kritische Gerade zu sein hängt offenbar nicht von der Wahl von S ab, sondern nur von der Richtung von g (s. 3.11 B)). Die Richtung einer kritischen Geraden nennt man entsprechend eine kritische Richtung von f.

B) Ist f nichtausgeartet, so gibt es wegen 3.10 a) genau eine Gerade g durch $S = (u_0, v_0)$, für die gilt

$$\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta = 0.$$

Diese Gerade nennen wir die *Tangente* zu f in S. Wir wollen uns überlegen, dass die Eigenschaft kritisch und Tangente zu sein sich gegenseitig ausschliessen, also:

a) *Die Gerade g kann nicht zugleich Tangente zu f in S und kritisch bezüglich f sein.*

Wäre dies nämlich der Fall, so hätten wir gemäss 3.10 b) die Gleichheit $\alpha = \beta = 0$, entgegen unserer Annahme, dass $(\alpha, \beta) \neq (0, 0)$. •

Aus der letzten Definition ist zunächst überhaupt nicht direkt ersichtlich, ob die Eigenschaft Tangente zu f zu sein unserer geometrischen Vorstellung einer Tangente entspricht. Ebenso leuchtet die geometrische Bedeutung der kritischen Gerade bezüglich f nicht ein. Auf beide Punkte werden wir später zu sprechen kommen. Als Konsequenz von 3.12 erhalten wir nun in der soeben eingeführten Sprechweise:

Korollar 3.14. *Seien $f, \mathbb{M}, S$ und g wie in 3.12. Dann gilt: Ist g kritisch bezüglich f oder die Tangente zu f in S, so ist S der einzige Schnittpunkt von $\mathbb{M}$ und g. Andernfalls haben $\mathbb{M}$ und g nebst S genau einen weiteren Schnittpunkt.* ■

Um die Bedeutung des vorangehenden Satzes zu schätzen sollte man wissen, ob es bezüglich einer Quadrik viele kritische Geraden geben kann. In der Tat kann es höchstens zwei solcher Geraden geben. Genauer gilt:

Satz 3.15. *Sei $f = Au^2 + Buv + Cv^2 + Du + Ev + F$ eine nichtausgeartete Quadrik, sei $S = (u_0, v_0) \in \mathbb{M}(f)$ und sei $\delta := B^2 - 4AC$. Dann gilt:*

a) *Ist $\delta < 0$, so gibt es keine bezüglich f kritische Gerade.*

b) *Ist $\delta = 0$, so gibt es genau eine bezüglich f kritische Gerade durch S. Die kritische Richtung ist dann festgelegt durch den gemäss 3.11 B) a) definierten Winkel*

$$\varphi = \begin{cases} \arctan\left(\frac{-B}{2C}\right), & \text{falls } C \neq 0; \\ \frac{\pi}{2}, & \text{falls } C = 0. \end{cases}$$

c) *Ist $\delta > 0$, so gibt es genau zwei bezüglich f kritische Geraden durch S. Die kritischen Richtungen sind dann festgelegt durch die Winkel*

$$\varphi = \begin{cases} \arctan(\frac{-B+\sqrt{\delta}}{2C}), & \text{falls } C \neq 0; \\ \frac{\pi}{2}, & \text{falls } C = 0, \end{cases}$$

$$\varphi' = \begin{cases} \arctan(\frac{-B-\sqrt{\delta}}{2C}), & \text{falls } C \neq 0; \\ \arctan(\frac{-A}{B}), & \text{falls } C = 0. \end{cases}$$

Beweis: Ist g eine kritische Gerade, so besteht in den Bezeichnungen von 3.11 die Gleichung $A\alpha^2 + B\alpha\beta + C\beta^2 = 0$. Aus dieser erhalten wir wegen $(\alpha, \beta) \neq (0, 0)$:

(α) $\alpha \neq 0 \Rightarrow \left(\frac{\beta}{\alpha}\right)^2 C + \left(\frac{\beta}{\alpha}\right) B + A = 0$;

(α') $\alpha = 0 \Rightarrow \beta \neq 0$ und $C = 0$.

Aus der Schule weiss man, dass die Gleichung

$$x^2 C + xB + A = 0$$

(β) keine Lösung hat, wenn $\delta < 0$;

(β') genau die Lösung $x = \frac{-B}{2C}$ hat, wenn $C \neq 0$ und $\delta = 0$;

(β'') genau die zwei Lösungen $x_{1/2} = \frac{-B\pm\sqrt{\delta}}{2C}$ hat, wenn $C \neq 0$ und $\delta > 0$.

„a)“: Ist $\delta < 0$, so ist $C \neq 0$. Mit $(\alpha), (\alpha')$ und (β) folgt sofort, dass es in diesem Fall keine kritische Gerade durch S gibt.

„b)“: Sei $\delta = 0$. Ist $C \neq 0$, so folgt aus $(\alpha), (\alpha')$ und (β'), dass es genau eine kritische Gerade durch S gibt, wobei $\alpha \neq 0$ und $\frac{\beta}{\alpha} = \frac{-B}{2C}$ gelten müssen. Ist $C = 0$, so folgt aus $\delta = 0$ auch $B = 0$. Weil f nichtausgeartet ist, folgt $A \neq 0$, also $\alpha = 0$ und es gibt wieder eine einzige kritische Gerade durch S. Die Aussage über den Winkel φ folgt nun mit 3.11 B) a).

„c)“: Sei $\delta > 0$. Ist $C \neq 0$, so folgt aus $(\alpha), (\alpha')$ und (β''), dass es genau zwei kritische Geraden durch S gibt, wobei für diese gilt $\frac{\beta}{\alpha} = \frac{-B\pm\sqrt{\delta}}{2C}$.

Ist $C = 0$, so gilt wegen $\delta > 0$ sicher $B \neq 0$, und die möglichen kritischen Geraden g durch S sind festgelegt durch die Lösungspaare (α, β) der Gleichung $A\alpha^2 + B\alpha\beta = 0$. Dies führt wieder zu genau zwei kritischen Geraden g durch den Punkt S. Für die eine dieser Geraden ist $\alpha = 0$, für die andere ist $\alpha \neq 0$ und $\frac{\beta}{\alpha} = -\frac{A}{B}$. ■

Geometrische Bedeutung der Tangenten und der kritischen Geraden

Wie schon früher angekündigt, möchten wir uns nun auch mit der anschaulich-geometrischen Seite des Begriffs der kritischen Geraden und der Tangenten auseinandersetzen.

Bemerkung 3.16. A) Sei $f(u, v) = Au^2+Buv+Cv^2+Du+Ev+F$ eine nichtausgeartete Quadrik und sei $S = (u_0, v_0) \in \mathbb{M}(f)$. Wir wählen $\tau \in \mathbb{R}$, setzen $\alpha = \cos(\tau)$ und $\beta = \sin(\tau)$ und betrachten die zugehörige Gerade g, definiert durch die Parameterdarstellung $s \mapsto (u_0 + \cos(\tau)s, v_0 + \sin(\tau)s)$ (s. 3.11 A) a)). Wir bezeichnen diese Gerade mit g_τ. Durchläuft τ das Intervall $\left]-\frac{\pi}{2}, \frac{\pi}{2}\right]$ (oder sogar ganz $\mathbb{R}$), so durchläuft g_τ alle möglichen Geraden durch S.

Sei zunächst τ so gewählt, dass g_τ weder Tangente zu f noch kritische Gerade bezüglich f ist. Gemäss 3.14 hat dann $\mathbb{M} = \mathbb{M}(f)$ mit g_τ nebst S genau einen weiteren Schnittpunkt, den wir mit $S_{[\tau]}$ bezeichnen wollen. Wegen $\sqrt{\cos(\tau)^2 + \sin(\tau)^2} = 1$ erhalten wir aus 3.12 und 3.11 B) b) (mit $\alpha = \cos(\tau)$ und $\beta = \sin(\tau)$) für die Distanz der beiden Punkte S und $S_{[\tau]}$ den Wert

a) $$\operatorname{dist}(S, S_{[\tau]}) = \left| \frac{\frac{\partial f}{\partial u}(u_0,v_0)\cos(\tau)+\frac{\partial f}{\partial v}(u_0,v_0)\sin(\tau)}{A\cos(\tau)^2+B\cos(\tau)\sin(\tau)+C\sin(\tau)^2} \right|$$

B) Sei nun $\psi \in]-\frac{\pi}{2}, \frac{\pi}{2}]$ der Richtungswinkel der Tangente zu f in S, d.h. g_ψ ist die Tangente zu f in S. Dann ist ψ sicher keine kritische Richtung bezüglich f (s. 3.13 B) a)). Also ist

$$N := A\cos(\psi)^2 + B\cos(\psi)\sin(\psi) + C\sin(\psi)^2 \neq 0.$$

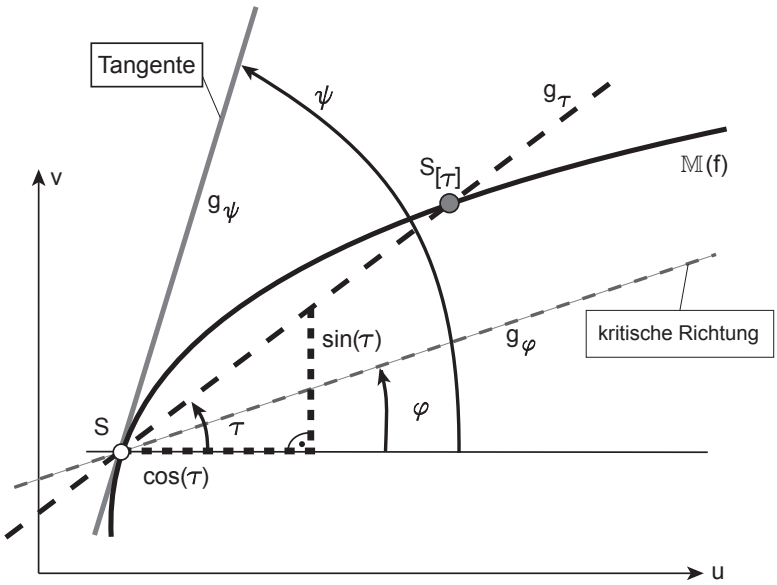


Abbildung 3.7: Tangente und kritische Gerade

Andererseits ist

$$\frac{\partial f}{\partial u}(u_0, v_0)\cos(\psi) + \frac{\partial f}{\partial v}(u_0, v_0)\sin(\psi) = 0.$$

Lassen wir τ (in $\mathbb{R}\backslash\{\psi + n\pi | n \in \mathbb{Z}\}$) nach ψ streben, so strebt der Zähler des in A) a) rechts stehenden Bruches nach 0, während der Nenner nach $N \neq 0$ strebt, denn sowohl der Zähler als auch der Nenner sind stetige Fuktionen in τ. Es gilt deshalb

$$\lim_{\tau \to \psi} \operatorname{dist}(S, S_{[\tau]}) = 0.$$

In Worten ausgedrückt: Dreht die Gerade g_τ zur Tangente g_ψ ein, so strebt der Schnittpunkt $S_{[\tau]}$ von g_τ mit $\mathbb{M}$ gegen den Punkt S : g_τ wird im anschaulichen Sinne zur Tangente, wenn „g_τ zu g_ψ eindreht“.

C) Wir wählen nun $\varphi \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ so, dass g_φ eine kritische Gerade ist. Solche kritische Werte gibt es nach 3.15 höchstens zwei.

Nun ist aber (weil g_φ eine kritische Gerade ist)

$$A\cos(\varphi)^2 + B\cos(\varphi)\sin(\varphi) + C\sin(\varphi) = 0$$

und (weil g_φ gemäss 3.13 B) a) keine Tangente ist)

$$Z := \frac{\partial f}{\partial u}(u_0, v_0)\cos(\varphi) + \frac{\partial f}{\partial v}(u_0, v_0)\sin(\varphi) \neq 0.$$

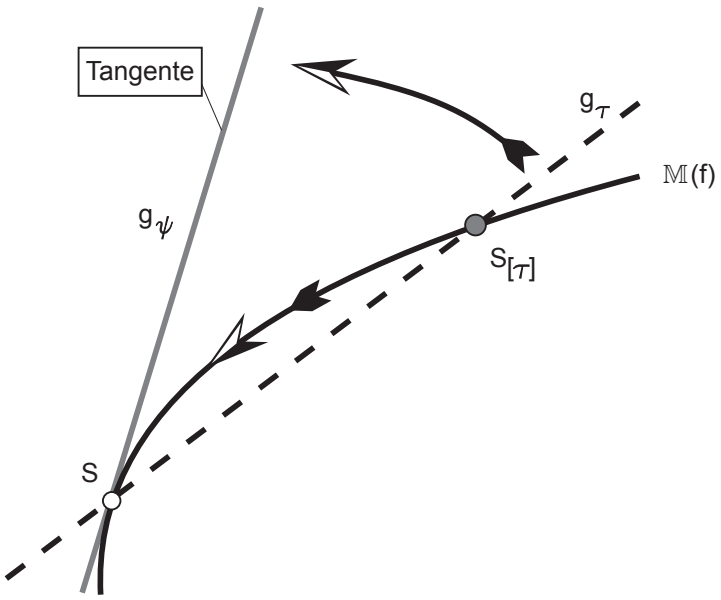


Abbildung 3.8: Grenzverhalten in Tangentenrichtung

Lässt man τ nach φ streben (unter Vermeidung der Werte $\varphi + n\pi$ und $\varphi' + n\pi$ ($n \in \mathbb{Z}$), wo $\varphi' \in \left]-\frac{\pi}{2}, \frac{\pi}{2}\right]$ die allfällige zweite kritische Richtung von f festlegt), so strebt der Zähler des in A) a) rechts stehenden Bruches nach Z, der Nenner aber nach 0. Es folgt

$$\lim_{\tau \to \varphi} \operatorname{dist}(S, S_{[\tau]}) = \infty.$$

In Worten ausgedrückt: Dreht die Gerade g_τ in eine kritische Richtung ein, so wandert der Schnittpunkt $S_{[\tau]}$ ins Unendliche ab. Die Kurve $\mathbb{M}(f)$ verschwindet also in der kritischen Richtung im Unendlichen.

D) Ohne weiteren Kommentar wollen wir festhalten, was die vorangehenden Überlegungen im Fall $\mathbb{M}(f) \neq \emptyset$ nahelegen:

a) *Ist $B^2 - 4AC < 0$, d.h. gibt es keine bezüglich f kritische Gerade, so ist $\mathbb{M}(f)$ eine Ellipse.*

b) *Ist $B^2 - 4AC = 0$, d.h. gibt es genau eine bezüglich f kritische Richtung, so ist $\mathbb{M}(f)$ eine Parabel, und die kritische Richtung ist die Achsenrichtung dieser Parabel.*

c) *Ist $B - 4AC > 0$, d.h. gibt es genau zwei bezüglich f kritische Richtungen, so ist $\mathbb{M}(f)$ eine Hyperbel und, die kritischen Richtungen sind die Asymptotenrichtungen dieser Hyperbel.*

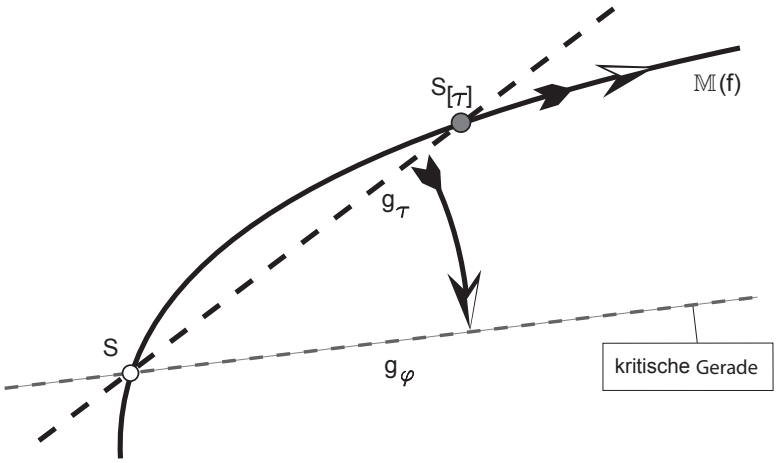


Abbildung 3.9: Grenzverhalten in kritischer Richtung

Wenn Sie finden, dass die Überlegungen aus A)–C) diese Aussagen nahelegen, so wissen Sie bereits, was Ellipsen, Parabeln und Hyperbeln sind. In diesem Fall fühlen Sie sich vielleicht herausgefordert, die Aussagen a), b) und c) zu beweisen. Sollte letzteres zutreffen, wäre ein Blick auf die Frage **??** (sinngemäss abgewandelt) vielleicht angezeigt. Sind für Sie Ellipsen, Parabeln, Hyperbeln und deren Eigenschaften hingegen Neuland, so können Sie die Aussagen a), b) und c) als Definition der neuen Begriffe verstehen. •

Aufgaben 3.17. A) Bestimmen Sie eine Parameterdarstellung und den Richtungswinkel der Tangente g zur Quadrik $f(u,v) = u^2+4v^2-4$ im Punkt $(u_0, v_0) = (u_0, ?)$ mit $v_0 > 0$.

B) Bestimmen Sie die kritischen Richtungen der Quadrik $-4u^2 + v^2 - 4 = f(u,v)$. Skizzieren Sie die Situation.

C) Sei $f(u,v) = u^2-2uv+v^2+u-1$. Zeigen Sie, dass f nichtausgeartet ist und bestimmen Sie die kritischen Richtungen von $f = f(u,v)$. Bestimmen Sie $(u_0, v_0) = S \in \mathbb{M} = \mathbb{M}(f)$ so, dass die Tangente zu f in S senkrecht zu einer kritischen Richtung verläuft.

D) Sei $f = f(u,v)$ eine nichtausgeartete Quadrik. Sei $h \subseteq \mathbb{R}^2$ eine Gerade. Zeigen Sie:

a) $\sharp\mathbb{M}(f) \cap h \leq 2$;

b) $\sharp\mathbb{M}(f) \cap h = 1$ gilt genau dann, wenn h kritisch oder eine Tangente zu f ist;

c) h kann nicht gleichzeitig Tangente und kritisch sein.

E) Sei $f = f(u,v)$ wie in C). Skizzieren Sie für $c \in \{0, \pm 1, \pm 2\}$ die Niveaulinien von $f(u,v) = c$. •

Rationale Parametrisierung der Quadriken

Nun führen wir die in 3.2 skizzierte Konstruktion auch wirklich aus.

Konstruktion 3.18. A) Sei $f(u,v) = Au^2 + Buv + Cv^2 + Du + Ev + F$ eine nichtausgeartete Quadrik. Sei $S = (u_0, v_0) \in \mathbb{M} = \mathbb{M}(f)$. Nach 3.10 a) sind dann die beiden partiellen Ableitungen $\frac{\partial f}{\partial u}(u_0, v_0)$ und $\frac{\partial f}{\partial v}(u_0, v_0)$ nicht beide 0. Wir wählen nun zwei Zahlen $a, b \in \mathbb{R}$ mit

$$\frac{\partial f}{\partial u}(u_0, v_0)a + \frac{\partial f}{\partial v}(u_0, v_0, v_0)b = 0 \text{ und } (a,b) \neq (0,0).$$

Eine Wahl, die sich aufdrängt, ist natürlich etwa (s. auch 3.8 C) a), b)):

a) $a := \frac{\partial f}{\partial v}(u_0, v_0) + 2Cv_0 + Bu_0 + E;$

$b := -\frac{\partial f}{\partial u}(u_0, v_0, v_0) = -(2Au_0 + Bv_0 + D).$

Nun betrachten wir die Hilfsgerade h, gegeben durch die Parameterdarstellung

b) $h : t \mapsto P_t := (u_0 + b + at, v_0 - a + bt).$

Gemäss 3.13 B) wird die Tangente zu f in S parametrisiert durch $t \mapsto (u_0 + at, v_0 + bt)$ und hat damit den gleichen Richtungsvektor wie die Gerade h, nämlich (a, b). Damit ist h parallel zur Tangente oder fällt mit dieser zusammen. Für jede Wahl von t gilt aber auch

$$\begin{aligned} \operatorname{dist}(S, P_t) &= \sqrt{(b+at)^2 + (-a+bt)^2} \\ &= \sqrt{a^2 + a^2t^2 + b^2 + b^2t^2} = \sqrt{a^2(1+t^2) + b^2(1+t^2)} \\ &= \sqrt{1+t^2}\sqrt{a^2+b^2} \geq \sqrt{a^2+b^2} > 0, \end{aligned}$$

also $S \neq P_t$. Dies bedeutet aber, dass $S \notin h$. Deshalb ist h nicht die Tangente zu f in S.

B) Wegen $S \neq P_t$ für alle $t \in \mathbb{R}$ gibt es zu jeder Zahl $t \in \mathbb{R}$ eine eindeutig bestimmte Gerade durch die Punkte S und P_t, die wir mit g_t bezeichnen. Die Gerade g_t parametrisieren wir nun gemäss 3.11 A) a) durch

$$g_t : s \mapsto (u_0 + \alpha(t)s, v_0 + \beta(t)s),$$

wobei

a) $\alpha(t) := b + at; s\beta(t) := -a + bt.$

Wegen $S, P_t \in g_t, S \notin h$ und $P_t \in h$ ist g_t sicher nicht parallel zu h, also auch nicht parallel zur Tangente zu f in S.

C) Ist g_t eine bezüglich f kritische Gerade, d.h. gilt (s. 3.13 A))

$$A\alpha(t)^2 + B\alpha(t)\beta(t) + C\beta(t)^2 = 0,$$

so nennen wir t einen *kritischen Parameterwert*. Da es höchstens zwei kritische Geraden gibt, kann es höchstens zwei kritische Parameterwerte geben. Wir schreiben $\mathcal{C}$ für die Menge dieser kritischen Parameterwerte, also

$$\mathcal{C} := \{t \in \mathbb{R} \,\big|\, A\alpha(t)^2 + B\alpha(t)\beta(t) + C\beta(t)^2 = 0\},$$

und vergessen nicht, dass $\sharp\mathcal{C} \leq 2$.

Nun wählen wir $t \in \mathbb{R}\backslash\mathcal{C}$. Dann ist g_t bezüglich f nicht kritisch und hat deshalb mit $\mathbb{M}$ nebst S noch genau einen weiteren Schnittpunkt $S_t := S_{g_t}$, der gemäss 3.12 b) gegeben ist durch

a) $$S_t = (u_0 - s(t)\alpha(t),\ v_0 - s(t)\beta(t)),$$

wobei

b) $$s(t) = \frac{\frac{\partial f}{\partial u}(u_0,v_0)\alpha(t) + \frac{\partial f}{\partial v}(u_0,v_0)\beta(t)}{A\alpha(t)^2 + B\alpha(t)\beta(t) + C\beta(t)^2}.$$

Anschaulich präsentiert sich die Situation (im Fall wo $\mathbb{M}$ eine Hyperbel ist) wie in Abbildung 3.10 dargestellt.

D) Um zu einer „parameterfreien“Beschreibung unserer Konstruktion zu gelangen, beachten wir, dass die Parametrisierung $t \mapsto P_t$ von h (vgl. A) b)) eine bijektive Abbildung ist. Zu jedem Punkt $P \in h$ gibt es also genau einen Parameterwert $t \in \mathbb{R}$ mit $P_t = P$. Diesen Parameterwert bezeichnen wir mit $t(P)$. Es gilt also

$$P_{t(P)} = P.$$

Wir schreiben auch

$$g(P) := g_{t(P)}.$$

Ist $g(P)$ eine bezüglich f kritische Gerade, d.h. ist $t(P) \in \mathcal{C}$, so nennen wir $P \in h$ einen bezüglich f kritischen Punkt. Wegen $\sharp\mathcal{C} \leq 2$ gibt es höchstens 2 kritische Punkte auf h. Die Menge der nichtkritischen Punkte auf h bezeichnen wir mit h^0, also:

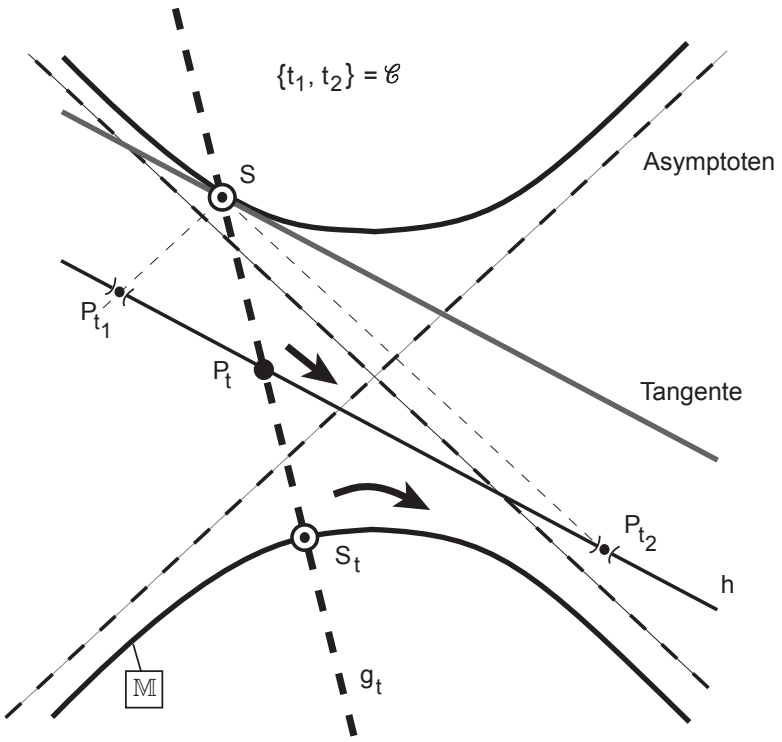


Abbildung 3.10: Konstruktion einer Parametrisierung

a) $h^0 := \{P \in h \,\big|\, t(P) \notin \mathcal{C}\}$.

Für $P \in h^0$ ist also $t(P)$ kein kritischer Parameterwert und wir können deshalb setzen:

b) $S(P) := S_{t(P)}, (P \in h^0)$.

Veranschaulicht an unserer Hyperbel $\mathbb{M}$ besteht nun also die Situation, die in Abbildung 3.11 dargestellt ist. •

Nun gelangen wir zum eigentlichen Hauptsatz dieses ganzen Kapitels, den wir zunächst wie folgt formulieren wollen:

Satz 3.19. *Es gelten die Voraussetzungen und Bezeichnungen aus 3.18. Dann besteht die bijektive Abbildung*

$$\sigma : h^0 \xrightarrow{\approx} \mathbb{M}\backslash\{S\};\ P \overset{\sigma}{\mapsto} S(P).$$

Beweis: Nach den Ausführungen in 3.18 ist $S(P) \in \mathbb{M}$ für alle $P \in h^0$ definiert, und von S verschieden. Also ist die angegebene Abbildung $\sigma : h^0 \to \mathbb{M}\backslash\{S\}$ überhaupt definiert.

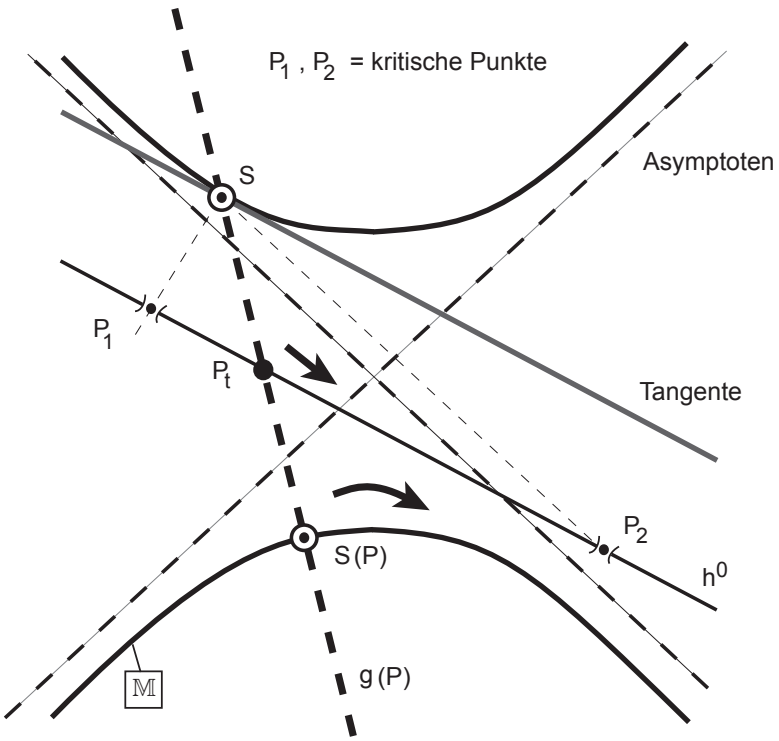


Abbildung 3.11: Parameterfreie Beschreibung der Konstruktion

Zuerst zeigen wir, dass σ injektiv ist. Seien also $P, Q \in h^0$ mit $\sigma(P) = \sigma(Q)$. Dann ist $S(P) = S(Q)$. Nun läuft aber $g(P)$ durch die Punkte S und $S(P)$, während $g(Q)$ durch die Punkte S und $S(Q)$ verläuft. Wegen $S(P) = S(Q) \neq S$ folgt $g(P) = g(Q)$. Nun sind aber P der Schnittpunkt von $g(P)$ mit h und Q der Schnittpunkt von $g(Q)$ mit h. Wegen $g(P) = g(Q)$ folgt $P = Q$. Damit ist gezeigt, dass σ injektiv ist.

Es bleibt zu zeigen, dass σ surjektiv ist. Sei also $T \in \mathbb{M}\backslash\{S\}$. Sei g die Gerade durch S und T. Weil g mit $\mathbb{M}$ mindestens die zwei verschiedenen Punkte S und T gemeinsam hat, kann g gemäss 3.16 weder kritisch bezüglich f noch die Tangente zu f in S sein. Weil h zu dieser Tangente parallel ist, folgt aus $S \in g$, dass h und g nicht parallel sind. Insbesondere schneidet g die Hilfsgerade h in einem einzigen Punkt P. Weil g bezüglich f nicht kritisch ist, gilt $P \in h^0$. Nun ist aber g die Gerade durch S und P, also $g = g(P)$. Weiter ist T der (nach 3.18 einzige) Schnittpunkt von $\mathbb{M}$ mit $g(P)$, der von S verschieden ist, also $T = S(P) = \sigma(P)$. Dies beweist, dass σ surjektiv ist. ■

Nun wollen wir den vorangehenden Satz in eine Form bringen, welche tatsächlich eine Parametrisierung der Menge $\mathbb{M}\backslash\{S\}$ ergibt.

Satz 3.20. *(Rationale Parametrisierung einer nichtausgearteten Quadrik) Sei* $f(u, v) = Au^2 + Buv + Cv^2 + Du + Ev + F$ *eine nichtausgeartete Quadrik und sei* $S = (u_0, v_0) \in$

$\mathbb{M} = \mathbb{M}(f)$. *Wir setzen*

$$\begin{aligned}
&a := 2Cv_0 + Bu_0 + E;\ b := 2Au_0 + Bv_0 + D;\\
&N(t) := -\Delta_f t^2 - (B(a^2 - b^2) - 2(A - C)ab)t + Ab^2 - Bab + ca^2;\\
&\mathcal{C} := \{t \in \mathbb{R} \,\big|\, N(t) = 0\};\\
&u(t) := u_0 + (a^2 + b^2)\frac{b + at}{N(t)}, (t \in \mathbb{R} \setminus \mathcal{C});\\
&v(t) := v_0 - (a^2 + b^2)\frac{a - bt}{N(t)}, (t \in \mathbb{R} \setminus \mathcal{C}).
\end{aligned}$$

Dann besteht die bijektive Abbildung

$$\varepsilon_S = \varepsilon : \mathbb{R}\backslash\mathcal{C} \xrightarrow{\approx} \mathbb{M}\backslash\{S\};\ t \mapsto \varepsilon(t) := (u(t), v(t)).$$

Beweis: In den Bezeichnungen von 3.18 A) a) und 3.18 B) a) gilt

$$\begin{aligned}
&A\alpha(t)^2 + B\alpha(t)\beta(t) + C\beta(t)^2\\
&= A(b + at)^2 + B(b + at)(-a + bt) + C(-a + bt)^2\\
&= (Aa^2 + Bab + Cb^2)t^2 + (2Aab - Ba^2 + Bb^2 - 2Cab)t\\
&+ Ab^2 - Bab + Ca^2.
\end{aligned}$$

Nach 3.18 A) a) und der Diskriminantenformel 3.9 gilt aber $Aa^2 + Bab + Cb^2 = -\Delta_f$ und es folgt

$$A\alpha(t)^2 + B\alpha(t)\beta(t) + C\beta(t)^2 = N(t).$$

Es gilt also tatsächlich

$$\mathcal{C} = \{t \in \mathbb{R} \,\big|\, t \text{ ist ein kritischer Parameterwert}\}.$$

Ist $t \in \mathbb{R}\backslash\mathcal{C}$, so gilt nun in den Bezeichnungen von 3.18 C) b) wegen 3.18 A) a) und 3.18 B) a) auch

$$s(t) = \frac{-b(b + at) + a(-a + bt)}{N(t)} = \frac{-b^2 - a^2}{N(t)},$$

also

$$s(t) = -\frac{a^2 + b^2}{N(t)}.$$

Vermöge 3.18 C) a) und 3.18 B) a) folgt also

$$S_t = \left(u_0 + \frac{a^2 + b^2}{N(t)}(b + at), v_0 + \frac{a^2 + b^2}{N(t)}(-a + bt)\right),$$

und damit

$$(\alpha) \qquad S_t = (u(t), v(t)),\ (t \in \mathbb{R}\backslash\mathcal{C}).$$

In den Bezeichnungen von 3.18 D) ist die Abbildung $t(\bullet) : h \to \mathbb{R}, (P \mapsto (t(P))$ bijektiv. Weiter gilt $t(h^0) = \mathbb{R}\backslash\mathcal{C}$, (s. 3.18 D) a)). Wir erhalten also die bijektive Abbildung

$$\psi : h^0 \xrightarrow{\approx} \mathbb{R}\backslash\mathcal{C};\ (P \mapsto t(P)).$$

Nach 3.18 D) b) und 3.19 gilt für alle $t \in \mathbb{R}\backslash\mathcal{C}$ die Beziehung

$$S_t = S_{\psi(\psi^{-1}(t))} = S_{t(\psi^{-1}(t))} = S(\psi^{-1}(t)) = \sigma(\psi^{-1}(t)).$$

Für die durch $t \mapsto S_t$ definierte Abbildung $\varepsilon : \mathbb{R}\backslash\mathcal{C} \to \mathbb{M}\backslash\{S\}$ gilt also

$$\varepsilon(t) = \sigma(\psi^{-1}(t)) = \sigma \circ \psi^{-1}(t);\ (t \in \mathbb{R}\backslash\mathcal{C}).$$

Damit ist ε die Komposition der bijektiven Abbildung ψ^{-1} mit der nach 3.19 ebenfalls bijektiven Abbildung σ. Also ist ε bijektiv, d.h. es besteht gemäss (α) tatsächlich die bijektive Abbildung

$$\varepsilon : \mathbb{R}\backslash\mathcal{C} \xrightarrow{\approx} \mathbb{M}\backslash\{S\};\ t \mapsto \varepsilon(t) = S(t) = (u(t), v(t)).$$

■

Für nichtausgeartete rationale Quadriken gilt nun die folgende wichtige Ergänzung:

Korollar 3.21. *Es gelten die Voraussetzungen und Bezeichnungen von 3.20. Zudem seien die Quadrik f rational (d.h. $A, B, C, D, E, F \in \mathbb{Q}$) und der Punkt $S \in \mathbb{M}$ rational (d.h. $u_0, v_0 \in \mathbb{Q}$). Weiter sei $t \in \mathbb{R}\backslash\mathcal{C}$. Dann gilt:*

$$t \in \mathbb{Q} \Longleftrightarrow \varepsilon(t) \in \mathbb{Q}^2.$$

Beweis: „$\Longrightarrow$“: Sei $t \in \mathbb{Q}$. Nach Voraussetzung gilt $A, B, C, D, E, F, u_0, v_0 \in \mathbb{Q}$. Es folgt $a, b \in \mathbb{Q}$. Wegen $t \in \mathbb{Q}$ folgt nun aber auch $N(t) \in \mathbb{Q}$ und $b - at, a + bt \in \mathbb{Q}$, d.h. $u(t), v(t) \in \mathbb{Q}$, also $\varepsilon(t) = (u(t), v(t)) \in \mathbb{Q}^2$.

„$\Longleftarrow$“: Sei $\varepsilon(t) \in \mathbb{Q}^2$. Dann gilt $u(t), v(t) \in \mathbb{Q}$. Wegen $u_0, v_0 \in \mathbb{Q}$ folgen $a, b, (a^2 + b^2)\frac{b+at}{N(t)}, (a^2 + b^2)\frac{a-bt}{N(t)} \in \mathbb{Q}$. Nach 3.10 a) ist $a \neq 0$ oder $b \neq 0$. Insbesondere ist $a^2 + b^2 \in \mathbb{Q}\backslash\{0\}$ und es folgt

$$(\alpha) \qquad \frac{b + at}{N(t)}, \quad \frac{a - bt}{N(t)} \in \mathbb{Q}.$$

Ist $a - bt = 0$, so folgt aus $(a, b) \neq (0, 0)$, dass $b \neq 0$, also, dass $t = \frac{a}{b} \in \mathbb{Q}$.

Sei also $a - bt \neq 0$. Durch Division der beiden Brüche aus (α) folgt dann $\frac{b+at}{a-bt} \in \mathbb{Q}$. Mit geeignetem $q \in \mathbb{Q}$ gilt also

$$\frac{b + at}{a - bt} = q,$$

d.h.

$$(\beta) \qquad b - aq = -(a + bq)t.$$

Ist $a + bq \neq 0$, so folgt aus $b - aq, a + bq \in \mathbb{Q}$, dass $t \in \mathbb{Q}$ und wir sind fertig.

Ist $a+bq = 0$, so ist gemäss (β) auch $b-aq = 0$, d.h. $b = aq$ und es folgt der Widerspruch $a^2 + b^2 = a^2 + abq = a(a + bq) = 0$. Also muss immer gelten $a + bq \neq 0$. ■

Als Anwendung ergibt sich:

Korollar 3.22. *Sei $f(u, v) = Au^2 + Buv + Cv^2 + Eu + Dv + F$ eine nichtausgeartete rationale Quadrik und sei $S = (u_0, v_0) \in \mathbb{M} = \mathbb{M}(f)$ mit $u_0, v_0 \in \mathbb{Q}$. Dann gilt in den Bezeichnungen von 3.20:*

a) *Durch Einschränkung der Abbildung $\varepsilon = \varepsilon_S : \mathbb{R}\backslash\mathcal{C} \to \mathbb{M}\backslash\{S\}$ erhält man eine bijektive Abbildung*

$$\varepsilon_S\restriction = \varepsilon\restriction : \mathbb{Q}\backslash\mathcal{C} \xrightarrow{\approx} \mathbb{Q}^2 \cap (\mathbb{M}\backslash\{S\}),\ (t \mapsto (u(t), v(t)).$$

b) $\mathbb{Q}^2 \cap \mathbb{M} = \{S\} \cup \{(u(t), v(t)) \,|\, t \in \mathbb{Q}\backslash\mathcal{C}\}$.

Beweis: „a)“: Weil $\varepsilon : \mathbb{R}\backslash\mathcal{C} \to \mathbb{M}\backslash\{S\}$ gemäss 3.20 bijektiv ist, folgt die Behauptung sofort aus 3.21.

„b)“: Klar aus Aussage a). ■

Definition 3.23. A) Sei $f(u, v) = Au^2+Buv+Cv^2+Du+Ev+F$ eine nichtausgeartete Quadrik und sei $S = (u_0, v_0) \in \mathbb{M} = \mathbb{M}(f)$. Die bijektive Abbildung

$$\varepsilon_S = \varepsilon : \mathbb{R}\backslash\mathcal{C} \xrightarrow{\approx} \mathbb{M}\backslash\{S\};\ (t \mapsto \varepsilon(t) = (u(t), v(t)))$$

aus 3.20 heisst die *zu S gehörige rationale (Standard-)Parametrisierung von f* (oder von $\mathbb{M}$).

B) Sei nun $f(u, v) = Au^2 + Buv + Cv^2 + Du + Ev + F$ eine nichtausgeartete rationale Quadrik und sei $S = (u_0, v_0) \in \mathbb{Q} \cap \mathbb{M}$ ein rationaler Punkt von $\mathbb{M}$. Die bijektive Abbildung

$$\varepsilon_S\restriction = \varepsilon\restriction : \mathbb{Q}\backslash\mathcal{C} \xrightarrow{\approx} \mathbb{Q}^2 \cap (\mathbb{M}\backslash\{S\});\ (t \mapsto \varepsilon(t) = (u(t), v(t))$$

aus 3.22 heisst dann die *zu S gehörige (Standard-)Parametrisierung der rationalen Punkte von f (oder von $\mathbb{M}$).* •

Unsere bisherigen Ausführungen mögen sehr technisch erscheinen. Ihre Quintessenz lässt sich aber in prägnanter Weise auch ohne viel algebraischen Apparat formulieren:

Hauptsatz 3.24. *Ist $f = f(u, v)$ eine nichtausgeartete rationale Quadrik und ist S ein rationaler Punkt von f, so können mit Hilfe der zu S gehörigen Standardparametrisierung von f alle rationalen Punkte von f beschrieben werden.* ■

Oder noch prägnanter

- *Kennt man einen einzigen rationalen Punkt einer nichtausgearteten rationalen Quadrik, so kennt man alle rationalen Punkte dieser Quadrik.*

Aufgaben 3.25. A) Skizzieren Sie die in Abbildungen 3.10 und 3.11 dargestellte Situation falls f

a) eine Ellipse ist (d.h. $\mathcal{C} = \emptyset$);

b) eine Parabel ist (d.h. $\sharp\mathcal{C} = 1$).

B) Bestimmen Sie die rationale Standard-Parametrisierung von $f(u, v)$ bezüglich $S = (u_0, v_0) \in \mathbb{M} = \mathbb{M}(f)$ falls

a) $f(u, v) = Au^2 + Cv^2 - 1$ mit $0 < A \leq C$ und $S = (0, 1/\sqrt{C})$;

b) $f(u, v) = Cv^2 - u - 1$ mit $C > 0$ und $S = (1-, 0)$;

c) $f(u, v) = Au^2 + Cv^2 - 1$ mit $A < 0 < C$ und $S = (0, 1/\sqrt{-A})$.

C) Sei $f(u, v) = Au^2 + Buv + Cv^2 + Du + Ev$ eine nichtausgeartete Quadrik. Bestimmen Sie die rationale Standard-Parametrisierung von f bezüglich $S = (0, 0)$.

D) Bestimmen Sie die rationale Standard-Parametrisierung der Quadrik $f = f(u, v) = u^2 + v^2 + u + v$ bezüglich $S = (0, 0)$ und beschreiben Sie damit $\mathbb{Q}^2 \cap \mathbb{M}(f)$.

E) Bestimmen Sie die rationale Standard-Parametrisierung der Quadrik $f = f(u, v) = u^2 - dv^2 - 1$ für $d \in \mathbb{N}$ bezüglich $s = (1, 0)$. Bestimmen Sie damit $\mathbb{Q}^2 \cap \mathbb{M}(f)$. Was lässt sich über $\mathbb{Z}^2 \cap \mathbb{M}(f)$ sagen? •

Kapitel 4

Rationale Punkte auf Kurven höheren Grades: Ein Ausblick

Überblick

In diesem letzten Kapitel wagen wir einen Ausblick auf die homogenen diophantischen Gleichungen vom Grad $n > 2$, wobei wir uns nach wie vor auf den Fall von drei Unbekannten beschränken. Wir werden die Bestimmung der ganzzahligen Lösungen einer solchen Gleichung auch in diesem Fall wieder auf das Aufsuchen rationaler Punkte auf gewissen ebenen Kurven zurückführen. Dieses Kapitel ist, wie schon in der Einleitung angekündigt, primär als eine Anleitung zum Selbststudium zu verstehen.
Aus diesem Grund legen wir vom 2. bis zum 4. Abschnitt das "algebraische Fundament" für unsere späteren Überlegungen. Wir konnten es nämlich nicht lassen, einige wichtige Grundresultate über Polynome (in einer oder zwei Variablen) zu behandeln, welche zum Verständnis der ebenen algebraischen Kurven unerlässlich sind. Wir empfehlen den interessierten Leserinnen und Lesern, sich diesen Vorbereitungsteil doch etwas eingehender anzueignen. Im Sinne einer Anleitung zum Selbststudium werden die meisten dieser Vorbereitungen in Form von Übungen präsentiert. In einigen wenigen Sätzen fassen wir das für die Behandlung unserer ebenen Kurven Unerlässliche zusammen. Die Beweise dieser Sätze werden aber bereits weitgehend in den Übungen vorweggenommen. Wir hoffen, dass wir auf diese Weise den Leserinnen und Lesern einen kleinen (wenn vielleicht auch nur auffrischenden) Vorgeschmack auf die algebraische Geometrie vermitteln (respetive wiedererwecken) können.
Währenddem sich die homogenen quadratischen Gleichungen im Prinzip (bis auf dass in Kapitel 2 erwähnte *Hasse-Prinzip*) mit den Hilfsmitteln der Schulmathematik vollständig "in den Griff bekommen lassen" erwartet uns bereits beim Übergang vom Grad zwei zum Grad drei ein gewaltiger "Quantensprung". Wir tauchen nämlich bei diesem Übergang mitten in die tiefsten und schwierigsten Probleme der zeitgenössischen mathematischen Forschung ein. Das heisst natürlich für uns, dass wir uns auf das Äusserste beschränken

müssen und lediglich gewisse einfach formulierbare Grundresultate präsentieren können. Besondere Bedeutung legen wir in diesem Kapitel auf den Fall $n = 3$. Dieser Fall führt uns in das Gebiet der *elliptischen Kurven*. Die elliptischen Kurven sind ein klassisches Thema der diophantschen Geometrie – ein Thema von aussergewöhnlicher Reichhaltigkeit und Schnheit. Leider ist es in diesem Kurs nicht möglich, die ausserordentlich wichtige Stellung dieses Gebietes und seine zahlreichen Verbindungen zu anderen Bereichen der Mathematik nur annähernd zur Darstellung zu bringen. Besonders erwähnen wollen wir, dass die Theorie der elliptischen Kurven auch heute noch mit zahlreichen ungelösten Problemen von ausserordentlichem Gewicht aufwartet.
Besonders wichtig ist, dass die elliptischen Kurven als abelsche Gruppen verstanden werden können. Sie sind damit Spezialfälle einer sehr wichtigen Klasse von algebraischen Varietäten, den sogenannten *abelschen Varietäten*.
Wir beschränken uns in diesem Kurs auf die Behandlung ellipischer Kurven in *affiner Normalform*. In diesem Fall lässt sich die Gruppenstruktur dieser Kurven besonders einfach und anschaulich beschreiben. Genau in dieser Situation werden wir dann auch die entsprechende *Gruppenstruktur* einführen – dabei allerdings den Nachweis der Assoziativität nicht erbringen. Dann werden wir den *Satz von Mordell* formulieren, der besagt, dass die rationalen Punkte einer elliptischen Kurve eine endlich erzeugte abelsche Gruppe bilden. Kurz werden wir dann auf das Problem der Bestimmung des *Ranges* und der *Torsionscharakteristik* einer elliptischen Kurve eingehen – und damit sehr tiefe Fragen ansprechen, die auch heute noch Gegenstand intensiver mathematischer Forschung sind.
Dann weisen wir auch auf den faszinierenden Zusammenhang hin, der zwischen der Theorie der elliptischen Kurven und dem bis heute einzigen als vollständig anerkannten Beweis der Fermat-Vermutung besteht – dem Beweis, der von Taylor und Wiles im Jahre 1995 erbracht wurde. Dazu ist es allerdings nötig, den Begriff der *Frey'schen elliptische Kurve* zu einem Tripel $(p, x, y) \in \mathbb{N}(p$ eine Primzahl > 2 einzuführen. Wir müssen aber auch von Modulfunktionen reden, um die *Modularitätsvermutung von Taniyama-Shimura* zu formulieren, welche recht eigentlich "das Scharnier" im Beweis der Fermat-Vermutung ist. Dies erlaubt uns dann auch, den *Nicht-Modularitätssatz von Ribet* für die Frey'schen elliptischen Kurven zu formulieren. Allerdings werden wir den für die Formulierung des *Modularitätssatzes von Taylor-Wiles* benötigten Begriff der *semistabilen elliptischen Kurve* nicht mehr einführen.
Nur am Rande weisen wir auch auf die Anwendung der (über endlichen Körpern definierten) elliptischen Kurven in der Kryptographie hin. Dies stellt uns in bemerkenswerter Weise ein Beispiel vor Augen, dass ein Gebiet der Mathematik, das lange Zeit als völlig "anwendungsfern" beurteilt wurde, sozusagen "über Nacht" von grösster Bedeutung für die Anwendungen werden kann.
Im letzten und sehr kurzen Unterabschnitt weisen wir auf den Fall hin, in welchem der Grad unserer homogenen diophantischen Gleichung > 3 ist. Hier formulieren wir (allerdings in einer sehr speziellen Situation) den wohl wichtigsten Satz der diophantischen Geometrie überhaupt. Es handelt sich um den *Satz von Faltings*, der vormaligen *Mordell-*

Vermutung aus dem Jahre 1922 – eine Vermutung, die bis zu ihrem Beweis im Jahre 1983 durch Faltings gemeinhin als die grösste Herausforderung der diophantischen Geometrie galt. Dieser Satz besagt in dem von uns formulierten Spezialfall, dass eine homogene diophantische Gleichung in drei Unbekannten und vom Grad ≥ 4 "im Wesentlichen" (d.h. in der *projektiven Ebene*) nur endlich viele Lösungen haben kann.

Es werden folgende Themen behandelt:

- *Homogene diophantische Gleichungen höheren Grades*,
- *Univariate Polynome*,
- *Bivariate Polynome*,
- *Kritische Geraden und Tangenten*,
- *Fernpunkte*,
- *Elliptische Kurven*,
- *Elliptische Kurven und die Fermat-Vermutung*,
- *Diophantische Formen vom Grad* > 3.

Homogene diophantische Gleichungen höheren Grades

In Kapitel 2 und 3 haben wir ausgiebig die homogenen quadratischen diophantischen Gleichungen studiert. In diesem Kapitel wagen wir nun den Blick auf homogene diophantische Gleichungen höheren Grades. Zunächst wollen wir das in den Definitionen 2.11 Gesagte verallgemeinern.

Definitionen 4.1. A) Sei $n \in \mathbb{N}$. Eine *diophantische Form vom Grad* n (oder eine *diophantische* n*-Form*) in den Unbestimmten x, y, z ist ein Polynom der Form

$$F(x,y,z) = \sum_{i,j \in \mathbb{N}_0 : i+j \leq n} a_{i,j} x^i y^j z^{n-i-j},$$

mit $a_{i,j} \in \mathbb{Q}$ für alle $i, j \in \mathbb{N}_0$ mit $i + j \leq n$, wobei mindestens einer der Koeffizienten $a_{i,j}$ von 0 verschieden ist. Sind alle koeffizienten $a_{i,j}$ von $F(x, y, z)$ ganze Zahlen, so nennen wir $F(x, y, z)$ eine *ganze diphantische* n*-Form*. Anstelle von $1, 2, 3, 4, 5, 6, \ldots$-Formen spricht man respektive auch von Quadriken, Kubiken, Quartiken, Quintiken, Sextiken, ...

B) Es gelten die Bezeichnungen aus Teil A). Wir sagen, die diophantische n-Form

$$F(x,y,z) = \sum_{i,j \in \mathbb{N}_0 : i+j \leq n} a_{i,j} x^i y^j z^{n-i-j}$$

sei *nichtausgeartet* die drei *partiellen Ableitungen* von $F(x,y,z)$ (s. Definition und Bemerkung 3.8) und $F(x,y,z)$ im Komplexen nur die triviale Nullstelle $(0,0,0)$ gemeinsam haben, das heisst, wenn für alle $(x_0,y_0,z_0)\in\mathbb{C}^3$ die folgende Implikation gilt:

$$\frac{\partial F}{\partial x}(x_0,y_0,z_0)=\frac{\partial F}{\partial y}(x_0,y_0,z_0)=\frac{\partial F}{\partial z}(x_0,y_0,z_0)=F(x_0,y_0,z_0)=0$$

$$\Longrightarrow x_0=y_0=z_0=0.$$

Eine *homogene diophantische Gleichung vom Grad n* in den Unbekannten x,y,z ist eine Gleichung der Form

$$F(x,y,z)=0,$$

in welcher $F(x,y,z)=\sum_{i,j\in\mathbb{N}_0:i+j\leq n}a_{i,j}x^iy^jz^{n-i-j}$ eine nichtausgeartete n-Form ist. Ist die n-Form zusätzlich ganz, so reden wir von einer *ganzen homogenen diophantischen Gleichung vom Grad n*.

Bemerkung und Definition 4.2. A) Sei $n\in\mathbb{N}$, sei

$$F(x,y,z)=\sum_{i,j\in\mathbb{N}_0:i+j\leq n}a_{i,j}x^iy^jz^{n-i-j},$$

eine diophantische n-Form und sei

$$F(x,y,z)=0$$

die zugehörige homogene diophantische Gleichung vom Grad n. Wir sind interssiert an den *nichttrivialen Lösungen* dieser Gleichung, d.h. an der Menge

(a) $\mathbb{L}(F):=\{(x_0,y_0,z_0)\in\mathbb{Z}^3\setminus\{(0,0,0)\}\mid F(x_0,y_0,z_0)=0\}$.

Ähnlich wie in Bemerkung 9.13 betrachten wir die drei Mengen

(b) $$\begin{cases}\mathbb{L}_x(F):=\{(x_0,y_0,z_0)\in\mathbb{L}(F)\mid x_0\neq 0\};\\ \mathbb{L}_y(F):=\{(x_0,y_0,z_0)\in\mathbb{L}(F)\mid y_0\neq 0\};\\ \mathbb{L}_z(F):=\{(x_0,y_0,z_0)\in\mathbb{L}(F)\mid z_0\neq 0\}.\end{cases}$$

B) Wir halten die obigen Bezeichnungen fest. Natürlich gilt auch hier wieder

$$\mathbb{L}(F)=\mathbb{L}_x(F)\cup\mathbb{L}_y(F)\cup\mathbb{L}_z(F),$$

sodass man sich ohne Einbusse an Allgemeinheit wieder darauf beschränken kann, nur eine der drei Teil-Lösungsmengen $\mathbb{L}_x(F),\mathbb{L}_y(F)$ oder $\mathbb{L}_z(F)$, zu studieren. Wir entscheiden uns willkürlich für die Untersuchung der dritten dieser Mengen, wie wir dies auch schon in Bemerkung 9.13 B) getan haben. Die in Bemerkung 2.8 vorgeschlagene – und

durch das Beispiel 1.7 inspirierte – Vorgehensweise lässt sich auch hier wieder anwenden. Entsprechend setzen wir als auch jetzt wieder

$$f = f(u,v) := F(u,v,1) = \sum_{i,j\in\mathbb{N}_0 : i+j\leq n} a_{i,j}u^i v^j$$

und

$$\mathbb{M}(f) = \mathbb{M}(f(u,v)) := \{(u_0,v_0) \in \mathbb{R}^2 \mid f(u_0,v_0) = 0\}.$$

Genauso wie in Bemerkung 2.13 C) können wir nun sagen:

$$\mathbb{L}_z(F) = \{(z_0u_0, z_0v_0, z_0) \mid (u_0,v_0) \in \mathbb{Q}^2 \cap \mathbb{M}(f), z_0 \in \mathbb{Z}\setminus\{0\} \text{ so, dass } z_0u_0, z_0v_0 \in \mathbb{Z}\}.$$

Insbesondere können wir uns also auch hier wieder darauf beschränken, anstelle der Menge $\mathbb{L}_z(F)$ die Menge $\mathbb{Q}^2 \cap \mathbb{M}(f)$ zu studieren.

Die folgenden Aufgaben zeigen, dass das, was wir in diesem Kapitel anstreben, eine Verallgemeinerung unserer Betrachtungen über lineare und quadratische diophantische Gleichungen ist.

Aufgaben 4.3. A) Zeigen Sie, dass eine diophantische 1-Form $F = F(x,y,z)$ immer nichtausgeartet ist und beschreiben Sie mit Hilfe des in Kapitel 1 behandelten Stoffes ein Lösungsverfahren für eine beliebige ganze homogene diphantische Gleichung $F(x,y,z) = 0$ vom Grad 1 in den Unbekannten x,y,z – d.h. ein Verfahren zur Bestimmung der Lösungsmenge $\mathbb{L}_z(F)$.

B) Zeigen Sie, dass die nichtausgearteten homogenen diophantischen Quadriken (s. Definitionen 2.11) in den Unbestimmten x,y,z gerade die nicht-ausgearteten ganzen diophantischen 2-Formen in diesen Unbestimmten sind.

C) Sei $F(x,y,z) = \sum_{i,j\in\mathbb{N}_0 : i+j\leq n} a_{i,j}x^i y^j z^{n-i-j}$ eine nichtausgeartete diophantische n-Form und sei

$$f = f(u,v) := F(u,v,1) = \sum_{i,j\in\mathbb{N}_0 : i+j\leq n} a_{i,j}x^i y^j.$$

Beweisen Sie als erstes die *Euler-Formel*

$$x\frac{\partial F}{\partial x}(x,y,z) + y\frac{\partial F}{\partial y}(x,y,z) + z\frac{\partial F}{\partial z}(x,y,z) = nF(x,y,z).$$

Wenden Sie diese Formel mit $z = 0$ an, um zu zeigen:

$$F(x,y,z) \text{ ist kein Vielfaches von } z.$$

Schliessen Sie daraus, dass

$$\mathrm{Grad}(f(u,v)) = n.$$

Zeigen Sie, dass

$$\frac{\partial F}{\partial x}(u,v,1) = \frac{\partial f}{\partial u}(u,v) \text{ und } \frac{\partial F}{\partial y}(u,v,1) = \frac{\partial f}{\partial v}(u,v).$$

Sei weiter $(u_0, v_0) \in \mathbb{M}(f)$. Beweisen Sie die folgende Eigenschaft der beiden partiellen Ableitungen von $f(u,v)$ im Punkt (u_0, v_0):

$$\big(\frac{\partial f}{\partial u}(u_0,v_0), \frac{\partial f}{\partial v}(u_0,v_0)\big) \neq (0,0).$$

D) Stellen Sie klar, dass es zu jeder homogenen diophantischen Gleichung $F(x,y,x)$ vom Grad n in den Unbekannten x, y, z eine ganze homogenen Diophantische Gleichung $\overline{F}(x,y,z) = 0$ vom Grad n in den Umbekannten x, y, z gibt so, dass

$$\mathbb{L}(F) = \mathbb{L}(\overline{F}).$$

Für Leserinnen und Leser, welche unsere weiteren Betrachtungen selbständig vertiefen wollen, lassen wir nun einige Dinge folgen, welche zur oben angeregten Untersuchung der Mengen $\mathbb{Q}^2 \cap \mathbb{M}(f)$ hilfreich sind.

Univariate Polynome

Wir beginnen mit einigen Vorbereitungen über *univariate Polynome*, d.h. Polynome in einer einzigen Variablen t.

Definition und Bemerkung 4.4. A) Wir bezeichnen wie üblich den *Körper der komplexen Zahlen* mit $\mathbb{C}$ und erinnern uns an die Inklusionen $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Ist $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, so schreiben wir

$$\mathbb{K}[t] := \{\sum_{i=0}^{d} a_i t^i \mid d \in \mathbb{N}_0 \text{ und } a_i \in \mathbb{K} \text{ für } i = 0, \ldots, d\}$$

für die Menge der *Polynome* in der *Unbestimmten* t und mit Koeffizienten in $\mathbb{K}$. Die Menge $\mathbb{K}[t]$ bildet bezüglich der üblichen Addition und Multiplikation von Polynomen einen kommutativen Ring. Deshalb nennen wir diese Menge auch den *Polynomring in* t *über (dem Koeffizientenkörper)* $\mathbb{K}$. Ist

$$f = f(t) = \sum_{i=0}^{d} a_i t^i \in \mathbb{K}[t],$$

so definieren wir den *Grad* von f durch

$$\mathrm{Grad}(f) = \mathrm{Grad}(f(t)) := \begin{cases} \max\{i \in \{0,\ldots,d\} \mid a_i \neq 0\}, & \text{wenn } f \neq 0 \\ -\infty, & \text{wenn } f = 0. \end{cases}.$$

Wichtig ist die *Additivität des Grades*, d. h. die Beziehung

$$\mathrm{Grad}(f(t)g(t)) = \mathrm{Grad}(f(t)) + \mathrm{Grad}(g(t)), \text{ für alle } f(t), g(t) \in \mathbb{K}[t],$$

wobei für alle $n \in \mathbb{Z} \cup \{-\infty\}$ die naheliegende Konvention $-\infty + n = n + (-\infty) = -\infty$ gelten soll. Natürlich gilt auch

$$\mathrm{Grad}(f(t) + g(t)) \leq \min\{\mathrm{Grad}(f(t)), \mathrm{Grad}(g(t))\} \text{ für alle } f(t), g(t) \in \mathbb{K}[t],$$

wobei Gleichheit besteht, wenn $\mathrm{Grad}(f(t)) \neq \mathrm{Grad}(g(t))$.
Weiter schreiben wir

$$\mathrm{Z}(f) = \mathrm{Z}_{\mathbb{K}}(f) = \mathrm{Z}_{\mathbb{K}}(f(t)) := \{z \in \mathbb{K} \mid f(z) = 0\}$$

und nennen diese Menge die *Nullstellenmenge* von f und ihre Elemente die *Nullstellen* von f.
Offenbar gelten folgende Aussagen:

(a) $\mathrm{Z}_{\mathbb{K}}(f) = \mathbb{K} \Leftrightarrow f = 0$;

(b) $f \in \mathbb{K} \setminus \{0\} \Rightarrow \mathrm{Z}_{\mathbb{K}}(f) = \emptyset$.

B) Seien $f(t), g(t) \in \mathbb{K}[t] \setminus \{0\}$ mit $\mathrm{Grad}(g(t)) \leq \mathrm{Grad}(f(t))$. Bekanntlich besagt dann der *Euklidsche Restsatz für Polynome*, dass es zwei eindeutig bestimmte Polynome $q(t), r(t) \in \mathbb{K}[t]$ so gibt, dass

$$\mathrm{Grad}(r(t)) < \mathrm{Grad}(g(t)) \text{ und } f(t) = g(t)q(t) + r(t).$$

In dieser Situation nennt man $q(t)$ den *Polynomquotienten* und $r(t)$ den *Divisionsrest* bei der Division von $f(t)$ durch $g(t)$.

C) Sei $f(t) \in \mathbb{K}[t]$ und sei $z \in \mathbb{K}$. Der *Satz von Vieta* besagt bekanntlich:

$$\text{Es gilt } z \in \mathrm{Z}_{\mathbb{K}}(f(t)) \text{ genau dann, wenn } f(t) = (t - z)q(t) \text{ für ein } q(t) \in \mathbb{K}[t].$$

Dieser Satz folgt übrigens leicht, wenn man $g(t) := t - z$ setzt und den Euklidschen Restsatz für Polynome anwendet.
Ist $f(t) \in \mathbb{K}[t] \setminus \{0\}$, so folgt durch Induktion über den Grad von f aus dem Satz von Vieta leicht, dass $f(t)$ eine *vollständige Abspaltung von Linearfaktoren* erlaubt, also eine Darstellung der folgenden Form besitzt:

$$f(t) = q(t) \prod_{i=1}^{r} (t - z_i)^{m_i},$$

wobei $r \in \mathbb{N}_0$, $q(t) \in \mathbb{K}[t]$ mit $\mathrm{Z}_{\mathbb{K}}(q(t)) = \emptyset$, $m_i \in \mathbb{N}$ und die Elemente $z_i \in \mathbb{K}$ paarweise verschieden sind $(i = 1, \ldots, r\}$. Dabei sind $q(t)$, r und die Menge der Paare (z_i, m_i) eindeutig besimmt und es gelten die Beziehungen

$$\mathrm{Grad}(q(t)) + \sum_{i=1}^{r} m_i = \mathrm{Grad}(g) \text{ und } \{z_1, \ldots, z_r\} = \mathrm{Z}_{\mathbb{K}}(f).$$

Eine unmittelbare Konsequenz aus dieser Gleichheit ist die Beziehung:

$$\#\mathrm{Z}_{\mathbb{K}}(f(t)) \leq \mathrm{Grad}(f(t)) \text{ für alle } f(t) \in \mathbb{K}[t] \setminus \{0\}.$$

Ist $z \in \mathbb{K}$, so definieren wir die *Vielfachheit von z als Nullstelle von f* durch

$$\mu_z(f) = \mu_z(f(t)) := \begin{cases} \max\{m \in \mathbb{N}_0 \mid \exists g(t) \in \mathbb{K}[t] : f(t) = (t-z)^m g(t)\}, & \text{wenn } f \neq 0 \\ \infty, & \text{wenn } f = 0. \end{cases}$$

Ist $f(t) \neq 0$ und ist $f(t) = q(t) \prod_{i=1}^{r} (t - z_i)^{m_i}$ die oben eingeführte vollständige Abspaltung der Linearfaktoren, so können wir also sagen:

$$\mu_z(f) = \begin{cases} m_i, & \text{falls } z = z_i \\ 0, & \text{falls } z \notin \{z_1, \ldots, z_r\} = \mathrm{Z}_{\mathbb{K}}(f(t)). \end{cases}$$

Insbesondere gilt:

$$\sum_{z \in \mathbb{K}} \mu_z(f(t)) \leq \mathrm{Grad}(f(t)) \text{ für alle } f(t) \in \mathbb{K}[t] \setminus \{0\}.$$

D) Der Körper $\mathbb{C}$ der komplexen Zahlen ist nach dem *Fundamentalsatz der Algebra* bekanntlich *algebraisch abgeschlossen*. Das heisst:

$$\text{Ist } f(t) \in \mathbb{C}[t] \text{ mit } \mathrm{Grad}(f(t)) \neq 0, \text{ so gilt } \mathrm{Z}_{\mathbb{C}}(f(t)) \neq \emptyset.$$

Für jedes Polynom $f(t) \in \mathbb{C}[t] \setminus \{0\}$ wird deshalb die in Teil C) angegebene vollständige Abspaltung von Linearfaktoren zur *vollständige Zerlegung in Linearfaktoren*, also zu einer Darstellung der Form

$$f(t) = c \prod_{i=1}^{r} (t - z_i)^{m_i},$$

mit $c \in \mathbb{C} \setminus \{0\}, z_i \in \mathbb{C}, m_i \in \mathbb{N}$ für $i = 1, \ldots, r$ und $z_i \neq z_j$ falls $i \neq j (i, j = 1, \ldots, r)$. Dabei sind c, r und die Menge der Paare (z_i, m_i) eindeutig besimmt und es gelten die Beziehungen

$$\sum_{i=1}^{r} m_i = \mathrm{Grad}(f(t)) \text{ und } \{z_1, \ldots, z_r\} = \mathrm{Z}_{\mathbb{C}}(f(t)).$$

Wir lassen nun einige Aufgaben über univariate Polynome folgen, welche unter anderem auch die späteren Betrachtungen vorbereiten sollen.

Aufgaben 4.5. A) Es gelten alle obigen Bezeichnungen. Sei $f = f(t) \in \mathbb{K}[t]$ und seien $z, z' \in \mathbb{K}$ und $c \in \mathbb{K} \setminus \{0\}$.

(a) $\mathrm{Grad}\big(f(t)\big) = \mathrm{Grad}\big(f(z' + ct)\big)$.

(b) $\mu_z(f(t)) = \mu_{\frac{z-z'}{\gamma}}\big(f(t_1 + ct)\big)$.

(c) Ist $g(t) \in \mathbb{C}[t]$ mit $f(t) = (t - z)g(t)$, so gilt $g(t) \in \mathbb{K}[t]$.

(d) Sind $g(t) \in \mathbb{C}[t]$ und $m \in \mathbb{N}_0$ mit $f(t) = (t - z)^m g(t)$, so folgt $g(t) \in \mathbb{K}[t]$.

(e) $\mu_z(f(t))$ ist unabhngig davon, ob man f als Polynom in $\mathbb{K}$ oder $\mathbb{C}$ auffasst.

(f) $\sum_{z \in \mathrm{Z}_{\mathbb{K}}(f(t))} \mu_z(f(t)) \leq \mathrm{Grad}(f(t))$ mit Gleichheit, wenn $\mathbb{K} = \mathbb{C}$.

B) Sei $r \in \mathbb{N}$, seien $z_1, \ldots, z_r \in \mathbb{R}$ und $m_1, \ldots, m_r \in \mathbb{N}$. Beschreiben Sie alle Polynome $f(t) \in \mathbb{R}[t]$ für welche gilt $\mathrm{Z}_{\mathbb{R}}(f(t)) = \{z_1, \ldots, z_r\}$, $\mu_{z_i}(f(t)) = m_i$ für alle $i = 1, \ldots, r$ und $\mathrm{Grad}(f(t)) = 2 + \sum_{i=1}^{r} m_i$.

C) Sei $f(t) = t^3 + a_2 t^2 + a_1 t + a_0 \in \mathbb{K}[t]$ vom Grad 3. Zeigen Sie, dass es ein eindeutig bestimmtes Element $\beta \in \mathbb{K}$ so gibt, dass für die neue Variable $\bar{t} := t + \beta$ gilt

$$f(t) = \overline{f}(\bar{t}) := \bar{t}^3 + a\bar{t} + b \in \mathbb{K}[\bar{t}] = \mathbb{K}[t].$$

Im folgenden Satz formullieren wir ein Resultat, das uns später hilfreich sein wird.

Satz 4.6. *Sei $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, sei $d \in \mathbb{N}$, sei $f(t) \in \mathbb{K}[t]$ vom Grad d und sei $Z \subset \mathrm{Z}_{\mathbb{K}}(f(t))$ so, dass $\sum_{z \in Z} \mu_z(f(t)) = d - 1$.*
Dann gibt es ein $z' \in \mathrm{Z}_{\mathbb{K}}(f(t)) \setminus Z$ so, dass

$$\mathrm{Z}_{\mathbb{K}}(f(t)) = Z \cup \{z'\} \text{ und } \mu_{z'}(f(t)) = 1.$$

Beweis. Nach dem, was wir alles in Definition und Bemerkung 4.4 C) gesehen haben, genügt es zu zeigen, dass $Z \neq \mathrm{Z}_{\mathbb{K}}(f(t))$. Nehmen wir an, es sei im Gegenteil $Z = \mathrm{Z}_{\mathbb{K}}(f(t))$. Dann findenh wir ein $r \in \mathbb{N}_0$ und paarweise verschiedene Elemente $z_1, \ldots, z_r$ so, dass $\{z_1, \ldots, z_r\} = Z = \mathrm{Z}_{\mathbb{K}}(f(t))$. Wir setzen $m_i := \mu_{z_i}(f(t))$. Nach Definition und Bemerkung 4.4 C) können wir dann schreiben

$$f(t) = q(t) \prod_{i=1}^{r} (t - z_i)^{m_i} \text{ mit } q(t) \in \mathbb{K}[t] \text{ und } \mathrm{Z}_{\mathbb{K}}(q(t)) = \emptyset.$$

Dabei ist nach Definition und Bemerkung 4.4 C) aber auch

$$\mathrm{Grad}(q(t)) = \mathrm{Grad}(f(t)) + \sum_{i=1}^{r} m_i = d - \sum_{z \in Z} \mu_z(f(t)) = 1$$

und wir erhalten daraus den Widerspruch, dass $\mathrm{Z}_{\mathbb{K}}(q(t)) \neq \emptyset$. □

Bivariate Polynome

Nun wollen wir uns auch den *bivariaten Polynomen* zuwenden, d.h. den Polynomen in zwei Variablen u, v.

Definition und Bemerkung 4.7. A) Sei wieder $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Wir schreiben

$$\mathbb{K}[u,v] := \{ \sum_{i,j \in \mathbb{N}_0 : i+j \leq n} a_{i,j} u^i v^j \mid n \in \mathbb{N}_0 \text{ und } a_{i,j} \in \mathbb{K} \text{ für } i,j \in \mathbb{N}_0 \text{ mit } i+j \leq n\}$$

für die Menge der *Polynome* in den *Unbestimmten* u und v mit Koeffizienten in $\mathbb{K}$. Bezüglich der üblichen Addition und Multiplikation von Polynomen ist $\mathbb{K}[u,v]$ ein kommutativer Ring. Wir nennen diesen Ring den *Polynomring in u und v über (dem Koeffizientenkörper)* $\mathbb{K}$. Ist

$$f = f(u,v) = \sum_{i,j \in \mathbb{N}_0 : i+j \leq n} a_{i,j} u^i v^j \in \mathbb{K}[u,v],$$

so definieren wir den *Grad* von f durch

$$\begin{aligned} \mathrm{Grad}(f) = \mathrm{Grad}(f(u,v)) := \\ := \begin{cases} \max\{i+j \mid i,j \in \mathbb{N}_0, i+j \leq n \text{ und } a_{i,j} \neq 0\}, & \text{wenn } f \neq 0 \\ -\infty, & \text{wenn } f = 0. \end{cases} \end{aligned}.$$

Wieder gilt die *Additivität des Grades*, d. h. die Beziehung

$$\mathrm{Grad}(f(u,v)g(u,v)) = \mathrm{Grad}(f(u,v)) + \mathrm{Grad}(g(u,v)), \text{ für alle } f(u,v), g(u,v) \in \mathbb{K}[u,v].$$

Natürlich gilt für alle $f(u,v), g(u,v) \in \mathbb{K}[u,v]$ auch

$$\mathrm{Grad}(f(u,v) + g(u,v)) \leq \min\{\mathrm{Grad}(f(u,v)), \mathrm{Grad}(g(u,v))\},$$

wobei auch hier wieder Gleichheit besteht, wenn $\mathrm{Grad}(f(u,v)) \neq \mathrm{Grad}(g(u,v))$.

B) Es gelten die Bezeichnungen aus teil A). Ähnlich wie im Fall univariater Polynome setzen wir

$$\mathrm{Z}(f) = \mathrm{Z}_{\mathbb{K}^2}(f) = \mathrm{Z}_{\mathbb{K}^2}(f(u,v)) := \{(u_0,v_0) \in \mathbb{K}^2 \mid f(u_0,v_0) = 0\}$$

und nennen diese Menge die *Nullstellenmenge* von f und ihre Elemente die *Nullstellen* von f. Offenbar gelten wieder folgende Aussagen:

(a) $\mathrm{Z}_{\mathbb{K}}(f) = \mathbb{K}^2 \Leftrightarrow f = 0$;

[b] $f \in \mathbb{K} \setminus \{0\} \Rightarrow \mathrm{Z}_{\mathbb{K}}(f) = \emptyset$.

C) Es gelten immer noch die obigen Bezeichnungen. Ist $f = f(u,v) \in \mathbb{R}[u,v]$, so verwenden wir schon in Bemerkung 2.8 B) eingeführte Bezeichnungsweise

$$\mathbb{M}(f) := \mathbb{M}(f(u,v)) := \mathrm{Z}_{\mathbb{R}^2}(f(u,v)) = \{(u_0,v_0) \in \mathbb{R}^2 \mid f(u_0,v_0) = 0\}.$$

Ist f vom Grad > 0 so nennen wir $\mathbb{M}(f)$ die *durch f in $\mathbb{R}^2$ definierte Kurve*, obwohl es vorkommen kann, dass diese Menge endlich ist. Die Bezeichnung "Kurve" bezieht sich darauf, dass,

$$\mathrm{Z}_{\mathbb{C}^2}(f) := \{(u_0,v_0) \in \mathbb{C}^2 \mid f(u_0,v_0) = 0\} \subset \mathbb{C}^2$$

im Sinne der algebraischen Geometrie eine *algebraische Kurve* ist, und dass wir schreiben können

$$\mathbb{M}(f) = \mathbb{R}^2 \cap \mathrm{Z}_{\mathbb{C}^2}(f).$$

Wir haben diese Sprechweise ja etwa schon in Beispiel 1.7 E) verwendet, als wir von den Fermatkurven sprachen.

Aufgaben 4.8. A) Seien $r \in \mathbb{N}_0$ und seien $(u_i, v_i) \in \mathbb{R}^2 \quad (i = 1, \dots r)$ paarweise verschiedene Punkte. Geben Sie ein Polynom $f \in \mathbb{R}[u,v]$ an so, dass

$$\mathrm{Grad}(f) = 2r \text{ und } \mathbb{M}(f) = \{(u_i,v_i) \mid i = 1, \dots, r\}.$$

B) Seien $f = f(u,v), g = g(u,v) \in \mathbb{R}[u,v]$. Zeigen Sie, dass

(a) $\mathbb{M}(fg) = \mathbb{M}(f) \cup \mathbb{M}(g)$.

(b) $\mathbb{M}(f^2 + g^2) = \mathbb{M}(f) \cap \mathbb{M}(g)$.

D) Sei $f(u,v) \in \mathbb{K}[u,v]$. Zeigen Sie, dass folgende Aussagen gelten:

(a) $\frac{\partial}{u}(u,v), \frac{\partial}{v}(u,v) \in \mathbb{K}[u,v]$.

(b) Sind $u_0, v_0 \in \mathbb{K}$ so gilt auch $\frac{\partial}{u}(u_0,v_0), \frac{\partial}{v}(u_0,v_0) \in \mathbb{K}$.

Definition und Bemerkung 4.9. A) Sei wieder $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Wir betrachten von neuem den Polynomring $\mathbb{K}[u,v]$ in u und v über $\mathbb{K}$. Ist $k \in \mathbb{N}_0$, so definieren wir die *k-te homogene Komponente* des Polynomringes $\mathbb{K}[u,v]$ durch:

$$\mathbb{K}[u,v]_{[k]} := \{ \sum_{i,j \in \mathbb{N}_0 : i+j \le n} a_{i,j} u^i v^j \in \mathbb{K}[u,v] \mid a_{i,j} = 0 \text{ für alle } i,j \in \mathbb{N}_0 \text{ mit } i+j \neq k\}.$$

Ein Polynom $f(u,v) \in \mathbb{K}[u,v]$ heisst *homogen*, wenn es ein $k \in \mathbb{N}_0$ so gibt, dass $f(u,v) \in \mathbb{K}[u,v]_{[k]}$. Ist dabei $f(u,v) \neq 0$, so gilt $\mathrm{Grad}(f(u,v)) = k$ und wir sagen, $f(u,v)$ sei *homogen vom Grad k*.

B) Es gelten weiterhin die obigen Bezeichnungen. Ist

$$f = f(u,v) = \sum_{i,j\in\mathbb{N}_0 : i+j\leq n} a_{i,j}u^i v^j \in \mathbb{K}[u,v],$$

und $k \in \mathbb{N}_0$, so definieren wir die *k-te homogene Komponente* von f als das homogene Polynom

$$f_{[k]} = f_{[k]}(u,v) := \sum_{i,j\in\mathbb{N}_0 : i+j=k} a_{i,j}u^i v^j = \sum_{l=0}^{k} a_{l,k-l}u^l v^{k-l} =$$
$$= \sum_{h=0}^{k} a_{k-h,h}u^{k-h}v^h \in \mathbb{K}[u,v]_{[k]} \subset \mathbb{K}[u,v].$$

Die resultierende eindeutige Summendarstellung

$$f = f(u,v) = \sum_{k=0}^{\mathrm{Grad}(f)} f_{[k]}(u,v) = \sum_{k=0}^{\mathrm{Grad}(f)} f_{[k]}$$

nennen wir die *Zerlegung von f in homogene Komponenten.*
Schliesslich definieren wir die *Leiftorm von f* durch:

$$\mathrm{LF}(f) = \mathrm{LF}(f(u,v)) := \begin{cases} f_{[\mathrm{Grad}f]} = f_{[\mathrm{Grad}(f(u,v))]}(u,v), & \text{wenn } f \neq 0 \\ 0, & \text{wenn } f = 0. \end{cases}$$

C) Ist $f(u) = \sum_{i=0}^{d} a_i u^i \in \mathbb{K}[u]$ vom Grad $d \geq 0$, so definieren wir die *Homogenisierung* von $f(u)$ bezüglich der Variablen v als das homogene Polynom

$$f(u)^{[v]} := \sum_{i=0}^{d} a_i u^i v^{d-i} \in \mathbb{K}[u,v]_{[d]}.$$

Die Homogenisierung $0^{[v]}$ des 0-Polynoms $0 \in \mathbb{K}[u]$ definieren wir als das 0-Polynom in $\mathbb{K}[u,v]$. Es gilt offensichtlich

$$\mathrm{Grad}(f(u))^{[v]} = \mathrm{Grad}(f(u)) \text{ für alle } f(u) \in \mathbb{K}[u].$$

Wie man leicht nachrechnet, ist die Homogenisierung auch *multiplikativ*, das heisst es gilt

$$\big(f(u)g(u)\big)^{[v]} = f(u)^{[v]}g(u)^{[v]} \text{ für alle } f(u), g(u) \in \mathbb{K}[u].$$

Wie man sofort nachprüft, gelten schliesslich auch die folgenden Aussagen:

(a) $f(u)^{[v]}(u,1) = f(u)$ für alle $f(u) \in \mathbb{K}[u]$.

(b) Ist $f(u,v) \in \mathbb{K}[u,v]$ homogen und kein Vielfaches von v, so gilt $f(u,v) = f(u,1)^{[v]}$.

Ist $f(v) = \sum_{i=0}^{d} a_i v^i \in \mathbb{K}[v]$ vom Grad d so kann man natürlich auch die Homogenisierung

$$f(v)^{[u]} = f(v)^{[u]}(u,v) := \sum_{i=0}^{r} a_i u^{d-i} v^i \in \mathbb{K}[u,v]_{[d]}$$

von $f(v)$ bezüglich u definieren, und erhält die entsprechnden Aussagen.

D) Sei $f(u,v) \in \mathbb{K}[u,v]_{[d]} \setminus \{0\}$. ein homogenes Polynom. Wir nehmen zuerst an, $f(u,v)$ sei kein Vielfaches von v. Gemäss Definition und Bemerkung 4.4 C) können wir dann in eindeutiger Weise schreiben

$$f(u,1) = q(u) \prod_{i=1}^{r} (u - z_i)^{m_i},$$

wobei $r \in \mathbb{N}_0$, $q(u) \in \mathbb{K}[u]$ mit $\mathrm{Z}_{\mathbb{K}}(q(u)) = \emptyset$, $m_i \in \mathbb{N}$ und die Elemente $z_i \in \mathbb{K}$ paarweise verschieden sind $(i = 1, \ldots, r\}$. Beachten wir nun die Aussage (b) aus Teil C) und die Multiplikativität der Homogenisierung, so erhalten wir

$$f(u,v) = f(u,1)^{[v]} = q(u)^{[v]} \prod_{i=1}^{r} \left((u - z_i)^{[v]}\right)^{m_i} = q(u)^{[v]} \prod_{i=1}^{r} (u - z_i v)^{m_i}.$$

Dabei ist das homogene Polynom $\mathrm{Z}(q(u)^{[v]})$ durch kein homogenes lineares Polynom der Form $(u - zv)$ teilbar. Denn sonst ergäbe sich ja – wegen $(z - z1) = 0$ und gemäss Aussage (a) aus Teil C) – der Widerspruch $q(z) = q(u)^{[v]}(z,1) = 0$.
Ist nun $f(u,v)$ allenfalls durch v teilbar, so schreiben wir $f(u,v) = v^s h(u,v)$, wobei $s \in \mathbb{N}_0$ und $h(u,v)$ nicht mehr durch v teilbar ist. Dann wenden wir das eben Gesagte auf das homogene Polynom $h(u,v)$ an. So erhalten wir dann eine *vollständige Abspaltung von homogenen Linearfaktoren* von $f(u,v)$, d.h. eine eindeutige Darstellung

$$f(u,v) = q(u,v) v^s \prod_{i=1}^{r} (u - z_i v)^{m_i},$$

in welcher $r, s \in \mathbb{N}_0$, $q(u,v) \in \mathbb{K}[u]$ homogen und durch kein homogenes Polynom vom Grad 1 teilbar ist – und wobei wieder $m_i \in \mathbb{N}$ und die Elemente $z_i \in \mathbb{K}$ paarweise verschieden sind $(i = 1, \ldots, r)$. Weil $q(u,v)$ homogen ist, folgt dann auch sofort, dass

$$\mathrm{Z}_{\mathbb{K}}(q(u,v)) \subset \{(0,0)\}.$$

Natürlich gilt dann

$$\mathrm{Grad}(q(u,v)) + \sum_{i=1}^{r} m_i = \mathrm{Grad}(f(u,v)).$$

E) Es gelten alle obigen Bezeichnungen. Ist $\mathbb{K} = \mathbb{C}$, so folgt aus Definition und Bemerkung 4.4 D), dass das in Teil C) eingeführte Polynom $q(u)$ zu $\mathbb{C} \setminus \{0\}$ gehört. Daraus folgt, dass die vorhin eingeführte vollständige Abspaltung homogener Linearfaktoren zur *vollständigen Zerlegung in Linearformen* wird. Es besteht also eine eindeutige Darstellung:

$$f(u,v) = cv^s \prod_{i=1}^{r} (u - z_i v)^{m_i},$$

in welcher $r, s \in \mathbb{N}_0$, $c \in \mathbb{C} \setminus \{0\}$, $m_i \in \mathbb{N}$ und die Elemente $z_i \in \mathbb{C}$ paarweise verschieden sind $(i = 1, \ldots, r)$. Insbesondere gilt nun

$$\sum_{i=1}^{r} m_i = \mathrm{Grad}(f(u,v)).$$

Aufgaben 4.10. A) Es gelten die obigen Bezeichnungen. Sei $f = f(u,v) \in \mathbb{K}[u,v]$. Zeigen Sie, dass folgende Aussagen gelten:

(a) $f_{[1]}(u,v) = \frac{\partial f}{\partial u}(0,0)u + \frac{\partial f}{\partial u}(0,0)v$.

(b) Sind $u_0, v_0 \in \mathbb{K}$ und fassen wir $\overline{f} = f(\overline{u}, \overline{v})$ als Polynom in den neuen Variablen $\overline{u} := u - u_0$ und $\overline{v} := v - v_0$ auf, so gelten die folgenden Beziehungen:

  (1) $\overline{f}(0,0) = f(u_0.v_0)$;
  (2) $\frac{\partial f}{\partial \overline{u}}(0,0) = \frac{\partial f}{\partial u}(u_0.v_0)$;
  (3) $\frac{\partial f}{\partial \overline{v}}(0,0) = \frac{\partial f}{\partial v}(u_0.v_0)$;
  (4) $\overline{f}_{[1]} = f_{[1]}(\overline{u}, \overline{v}) = \frac{\partial f}{\partial u}(u_0, v_0)\overline{u} + \frac{\partial f}{\partial u}(u_0, v_0)\overline{v}$.

B) Sei (u,v) wie in Teilaufgabe A) und seien $u_0, v_0 \in \mathbb{K}$. Zeigen Sie, dass es ein Polynom $r(u,v) \in \mathbb{K}[u,v]$ so gibt, dass

(a) $\mathrm{Grad}(r(u,v)) \leq \mathrm{Grad}(f(u,v))$;

(b) $r(u,v)_{[i]} = 0$ für $i = 0, 1$.

(c) $f(u,v) = f(u_0,v_0) + \frac{\partial f}{\partial u}(u_0,v_0)(u - u_0) + \frac{\partial f}{\partial u}(u_0,v_0)(v - v_0) + r(u - u_0, v - v_0)$.

C) Sei $n \in \mathbb{N}$. Bestimmen Sie alle rationalen Zahlen $a \in \mathbb{Q}$ derart, dass das homogene Polynom $f(u,v) := u^n + av^n$ einen homogenen Linearfaktor abspaltet.

Für sätere Zwecke halten wir den folgenden Auszug aus den vorangeheneen Überlegungen fest.

Satz 4.11. *Sei $n \in \mathbb{N}$, sei*

$$F(x,y,z) = \sum_{i,j\in\mathbb{N}_0: i+j\leq n} a_{i,j}x^i y^j z^{n-i-j}$$

eine nichtausgeartete diphantische n-Form. Dann gilt

$$f = f(u,v) := F(u,v,1) = \sum_{i,j\in\mathbb{N}_0: i+j\leq n} a_{i,j}u^i v^j \in \mathbb{Q}[u,v].$$

Zudem ist $\mathrm{Grad}(f(u,v)) = n$ *und für alle* $(u_0,v_0) \in \mathbb{M}(f(u,v))$ *gilt*

$$\big(\frac{\partial f}{\partial u}(u_0,v_0), \frac{\partial f}{\partial v}(u_0,v_0)\big) \neq (0,0).$$

Beweis. Dass $f(u,v) := F(u,v,1) = \sum_{i,j\in\mathbb{N}_0: i+j\leq n} a_{i,j}u^i v^j \in \mathbb{Q}[u,v]$, folgt sofort aus der Tatache, dass gemäss Definition der diophantischen n-Form $F(x,y,z)$ gelten muss $a_{i,j} \in \mathbb{Q}$ für alle $i,j \in \mathbb{N}_0$ mit $i+j \leq n$.
Die Gleichheit $\mathrm{Grad}(f(u,v)) = n$ und die obige Nichtverschwindungsaussage haben haben Sie bereits in Aufgabe 4.3 C) gezeigt. □

Kritische Geraden und Tangenten

Die bereits im Kapitel 3 für den Fall von Quadriken eingeführten Konzepte der Tangenten und der kritischen Geraden wollen wir nun auf beliebige nichtausgeartete diophantische n-Formen erweitern. Wir beginnen mit einigen vorbereitenden Aufgabe über Geraden.

Aufgaben 4.12. A) Die *Geraden* in $\mathbb{K}^2$ seien definiert als die Teilmengen der Form

$$g := \{(l(z),h(z)) \mid z \in \mathbb{K}\},$$

wobei $l = l(t) = \alpha t + u_0, h = h(t) = \beta t + v_0 \in \mathbb{K}[t]$ mit $\max\{\mathrm{Grad}(l), \mathrm{Grad}(h)\} = 1$.

In dieser Situation nennt man die Abbildung

$$\lambda : \mathbb{K} \longrightarrow g, \quad t \mapsto \lambda(t) = (l(t),h(t)) = (\alpha t + u_0, \beta t + v_0).$$

eine *lineare Parametrisierung von g*. Zeigen Sie

(a) Die lineare Parametrisierung $\lambda : \mathbb{K} \longrightarrow g, \quad t \mapsto \lambda(t) = (l(t),h(t))$ ist bijektiv.

(b) Die Geraden in $\mathbb{K}^2$ sind genau die Teilmengen der Form

$$\mathrm{Z}_{\mathbb{K}^2}(f(u,v)), \text{ wobei } f(u,v) \in \mathbb{K}[u,v] \text{ vom Grad 1 ist .}$$

(c) Ist $g = \mathrm{Z}_{\mathbb{K}^2}(f(u,v))$, wobei $f(u,v) \in \mathbb{K}[u,v]$ vom Grad 1 ist, so gilt $(0,0) \in g$ genau dann wenn $f(u,v)$ homogen ist.

B) Sei $d \in \mathbb{N}$ und sei $f(u,v) \in \mathbb{K}[u,v]_{[d]}$ homogen von Grad d so, dass $\mathrm{Z}_{\mathbb{K}^2}(f) \neq (0,0)$. Zeigen Sie, dass es eine Zahl $s \in \{0,\ldots,d\}$ und s paarweise verschiedene Geraden $g_1,\ldots,g_s \subset \mathbb{K}^2$ so gibt, dass

$$(0,0) \in g_i \text{ für } i = 1,\ldots,s \text{ und } \mathrm{Z}_{\mathbb{K}^2}(f(u,v)) = \bigcup_{i=1}^{s} g_i.$$

C) Sei $g \subset \mathbb{K}^2$ eine Gerade, versehen mit der *linearen Parametrisierung*

$$\lambda : \mathbb{K} \xrightarrow{\approx} g = \lambda(\mathbb{K}), \quad t \mapsto \lambda(t) := (l(t), h(t)),$$

wobei $l = l(t) = \alpha t + u_0, h = h(t) = \beta t + v_0 \in \mathbb{K}[t]$ mit $\max\{\mathrm{Grad}(l), \mathrm{Grad}(h)\} = 1$.

Wir setzen auch

$$\lambda_{[1]}(t) := (l_{[1]}(t), h_{[1]}(t)) = (\alpha t, \beta t) \text{ und } g' := \lambda_{[1]}(\mathbb{K}).$$

Natürlich ist $g' \subset \mathbb{K}^2$ die zu g parallele Gerade, die durch den Ursprung $\underline{0} = (0,0)$ läuft. Sei weiter $f = f(u,v) \in \mathbb{K}[u,v]$ vom Grad > 0. Zeigen Sie zuerst, dass

$$f\big(\lambda(t)\big) = f\big(l(t), h(t)\big), \quad f\big(\lambda_{[1]}(t)\big) = f\big(l_{[1]}(t), h_{[1]}(t)\big) \in \mathbb{K}[t].$$

Sei $P \in g$ und sei $z \in \mathbb{K}$ mit $P = \lambda(z)$. Zeigen Sie, mit Hilfe von Aufgabe 4.5 A) (a), (b), dass folgende Aussagen gelten:

(a) $\mathrm{Grad}\big(f(\lambda(t))\big)$ ist unabhängig von der gewählten linearen Parametrisierung λ von g, hängt also nur von f und g ab und erfüllt die Ungleichungen

$$\mathrm{Grad}\big(f(\lambda(t))\big), \mathrm{Grad}\big(f(\lambda_{[1]}(t))\big) \leq \mathrm{Grad}(f).$$

(b) Es sind äquivalent:

(i) $\mathrm{Grad}\big(f(\lambda(t))\big) < \mathrm{Grad}(f)$;

(ii) $\mathrm{Grad}\big(f(\lambda_{[1]}(t))\big) < \mathrm{Grad}(f)$;

(iii) $\mathrm{LF}(f)(\lambda_{[1]}(t)) = 0$;

(iv) $g' \subset \mathrm{Z}_{\mathbb{K}^2}\big(\mathrm{LF}(f)\big)$.

(c) $\mu_z\big(f(\lambda(t))\big)$ ist unabhängig von der gewählten linearen Parametrisierung λ von g, hängt also nur von f, g und P ab, und erfüllt die Ungleichung

$$\mu_z\big(f(\lambda(t))\big) \leq \mathrm{Grad}\big(f(\lambda(t))\big).$$

Im Weiteren wollen wir nun nur noch den Fall $\mathbb{K} = \mathbb{R}$ verfolgen.

Definition und Bemerkung 4.13. A) Sei $f(u,v) \in \mathbb{R}[u,v]$, sei $g \subset \mathbb{R}^2$ eine Gerade. Wir wählen eine lineare Parametrisierung $\lambda : \mathbb{R} \xrightarrow{\approx} g$ von g (s. Aufgabe 4.12 A)). Sei $P \in g$. Gemäss Aufgabe 4.12 C)(d) können wir die *Schnittvielfachheit von g mit f in P* definieren durch:

$$\mu_P(g, f(u,v)) := \mu_z\big(f(\lambda(t))\big), \text{ wobei } P = \lambda(z).$$

D) Es gelten die obigen Bezeichnungen. Gilt $\mu_P(g, f(u,v)) = 1$, so sagen wir g schneide $f(u,v)$ in P *transversal*.

C) Es gelten die vorangehenden Bezeichnungen. Gemäss Aufgabe 4.12 C)(a) können wir die *Schnittvielfachheit von g mit f im Unendlichen* definieren durch

$$\mu_\infty(g, f(u,v)) := \mathrm{Grad}(f(u,v)) - \mathrm{Grad}\big(\lambda(f(t))\big).$$

D) Es gelten die obigen Bezeichnungen. Nach Aufgabe 4.12 C)(b) besteht die logische Äquivalenz

$$\mu_\infty(g, f(u,v)) > 0 \Leftrightarrow g' \subset \mathbb{M}\big(\mathrm{LF}(f)\big),$$

wo $g' \subset \mathbb{R}^2$ wieder die durch $(0,0)$ laufende zu g parallele Gerade ist. Sind diese äquivalenten Bedingungen erfüllt, so nennen wir g eine bezüglich $f(u,v)$ *kritische Gerade*.

E) Es gelten die obigen Bezeichnungen. Auf Grund der Beziehung $\sum_{z\in\mathbb{R}} \mu_z(f(\lambda(t)) \leq \mathrm{Grad}\big(f(\lambda(t))\big)$ (s. Definition und Bemerkung4.4 C)) gilt

$$\mu_\infty(g, f(u,v)) + \sum_{P\in g} \mu_P(g, f(u,v)) \leq \mathrm{Grad}(f(u,v)).$$

Aufgaben 4.14. A) Sei $f(u,v) \in \mathbb{R}[u,v] \setminus \mathbb{R}$, sei $g \subset \mathbb{R}^2$ eine Gerade. Sei weiter $h \subset \mathbb{R}^2$ eine zu g parallele Gerade. Zeigen Sie, dass g bezüglich $f(u,v)$ kritisch ist, genau dann, wenn h bezüglich $f(u,v)$ kritisch ist.

B) Sei $f(u,v)$ wie in Aufgabe A), sei $r \in \mathbb{N}_0$ und seien $g_1, \ldots, g_r$ paarweise nicht-parallele Geraden, die bezüglich $f(u,v)$ kritisch sind. Zeigen Sie, dass $r \leq \mathrm{Grad}(f(u,v))$.

C) Sei $f(u,v)$ wie oben und sei $\underline{0} := (0,0) \in \mathbb{M}(f)$. Sei

$$m := \min\{i \in \mathbb{N}_0 \mid f_{[i]}(u,v) \neq 0\}$$

Zeigen Sie:

(a) Ist $m > 1$, so schneidet jede Gerade $g \subset \mathbb{R}^2$ mit $\underline{0} \in g$ das Polynom $f(u,v)$ in $\underline{0}$ nichttransversal.

(b) Ist $m = 1$, so ist $\mathbb{M}\big(f_{[1]}(u,v)\big)$ die einzige Gerade in $\mathbb{R}^2$, welche $f(u,v)$ in $\underline{0}$ nicht transversal schneidet.

D) Sei $f(u,v)$ definiert wie vorhin. Wir betrachten nun die beiden partiellen Ableitungen (s. Definition und Bemerkung 3.8)

$$\frac{\partial f}{\partial u}(u,v), \quad \frac{\partial f}{\partial v}(u,v) \in \mathbb{R}[u,v]$$

von $f(u,v)$. Beachten Sie die Aufgabe 4.10 A)(b) und zeigen Sie:

(a) Ist $\underline{0} = (0,0) \in \mathbb{M}(f)$ und $\big(\frac{\partial f}{\partial u}(0,0), \frac{\partial f}{\partial v}(0,0)\big) \neq (0,0)$, so ist

$$\mathbb{M}\big(\frac{\partial f}{\partial u}(0,0)u + \frac{\partial f}{\partial u}(0,0)v\big)$$

die einzige Gerade, welche $f(u,v)$ in $\underline{0}$ nicht transversal schneidet.

(b) Ist $P = (u_0, v_0) \in \mathbb{M}(f(u,v))$ und $\big(\frac{\partial f}{\partial u}(u_0,v_0), \frac{\partial f}{\partial v}(u_0,v_0)\big) \neq (0,0)$, so ist

$$\mathbb{M}\big(\frac{\partial f}{\partial u}(u_0,v_0)(u-u_0) + \frac{\partial f}{\partial u}(u_0,v_0)(v-v_0)\big)$$

die einzige Gerade in $\mathbb{R}^2$, welche $f(u,v)$ in P nicht transversal schneidet.

E) Sei $n \in \mathbb{N}$, sei

$$F(x,y,z) = \sum_{i,j \in \mathbb{N}_0 : i+j \leq n} a_{i,j} x^i y^j z^{n-i-j}$$

eine nicht ausgeartete diophantische n-Form und sei

$$f = f(u,v) := F(u,v,1) = \sum_{i,j \in \mathbb{N}_0 : i+j \leq n} a_{i,j} x^i y^j.$$

Zeigen Sie:

(a) $\frac{\partial F}{\partial z}(u,v,0) = f(u,v)_{[n-1]}$.

(b) $\frac{\partial F}{\partial x}(u,v,0) = \frac{\partial f_{[n]}}{\partial u}(u,v)$.

(c) $\frac{\partial F}{\partial y}(u,v,0) = \frac{\partial f_{[n]}}{\partial v}(u,v)$.

(d) $u\frac{\partial f_{[n]}}{\partial u}(u,v) + v\frac{\partial f_{[n]}}{\partial v}(u,v) = nf(u,v)_{[n]}$.

F) Sei $f(u,v) \in \mathbb{R}[u,v]$ eine nichtausgeartete Quadrik (s. Definition 3.5). Sei $g \subset \mathbb{R}^2$ eine Gerade und sei $(u_0, v_0) \in \mathbb{M}(f)$. Zeigen Sie:

(a) Die Gerade g ist genau dann kritisch bezüglich f im Sinne der Definition und Bemerkung 3.13 A), wenn Sie es im Sinne der Definition und Bemerkung 4.13 D) ist.

(b) Die Gerade g ist die Tangente zu f in P im Sinne der Definition und Bemerkung 3.13 B), wenn sie die einzige Gerade ist, welche $f(u,v)$ in P nicht transversal schneidet.

Bemerkung und Definition 4.15. Sei $F(x,y,z) = \sum_{i,j\in\mathbb{N}_0:i+j\leq n} a_{i,j}x^iy^jz^{n-i-j}$ eine nicht ausgeartete diophantische n-Form (s. Definition 4.1) und sei

$$f = f(u,v) := F(u,v,1) = \sum_{i,j\in\mathbb{N}_0:i+j\leq n} a_{i,j}x^iy^j.$$

Sei weiterhin $P = (u_0, v_0) \in \mathbb{M}(f)$. Nach Aufgabe 4.3 C) und Aufgabe 4.14 D)(b) wissen wir dann, dass

$$\mathbb{M}\big(\frac{\partial f}{\partial u}(u_0,v_0)(u-u_0) + \frac{\partial f}{\partial u}(u_0,v_0)(v-v_0)\big)$$

die einzige Gerade in $\mathbb{R}^2$ ist, welche $f(u,v)$ in P nicht transversal schneidet. Gerechtfertigt durch Aufgabe 4.14 E) nennen wir diese Gerade dann die *Tangente zu* $f = f(u,v)$ *in* P.

Nun wollen wir dem nächsten wichtigen Begriff zuwenden: dem Konzept der rationalen Geraden. Die folgende Übungsaufgabe dient als Vorbereitung.

Aufgaben 4.16. A) Sei $g \subset \mathbb{R}^2$ eine Gerade. Zeigen Sie, dass folgende Aussagen äquivalent sind:

(i) Es gibt zwei verschiedene Punkte $P, P' \in \mathbb{Q}^2 \cap g$.

(ii) $\#(\mathbb{Q}^2 \cap g) = \infty$.

(iii) Es gibt ein Polynom $f = f(u,v) \in \mathbb{Q}[u,v]$ vom Grad 1 derart dass $g = \mathbb{M}(f)$.

(iv) g besitzt eine *rationale lineare Parametrisierung*, d.h. es gibt zwei Polynome $l(t) = u_0 + \alpha t, h(t) = v_0 + \beta t \in \mathbb{Q}[t]$ mit $\max\{\mathrm{Grad}(l(t)), \mathrm{Grad}(h(t))\} = 1$ so, dass die folgende bijektive Abbildung besteht:

$$\lambda : \mathbb{R} \xrightarrow{\approx} g, \quad t \mapsto \lambda(t) := (l(t), h(t)) = (u_0 + \alpha t, v_0 + \beta t)$$

B) Es gelten die Bezeichnungen von A) und es seien

$$l(t), h(t) \in \mathbb{Q}[t] \text{ mit } \max\{\mathrm{Grad}(l(t)), \mathrm{Grad}(h(t))\} = 1.$$

Wir betrachten die Abbildung

$$\lambda : \mathbb{R} \longrightarrow \mathbb{R}^2, \quad t \mapsto \lambda(t) := (l(t), h(t)) \text{ für alle } t \in \mathbb{R}.$$

Zeigen Sie, dass folgende Bedingungen äquivalent sind:

(i) Es besteht die Bijektion $\lambda : \mathbb{R} \xrightarrow{\approx} g$.

(ii) Es besteht die Bijektion $\lambda \restriction: \mathbb{Q} \xrightarrow{\approx} \mathbb{Q}^2 \cap g$.

(iii) Es gilt $\lambda(\mathbb{R}) = g$.

(iv) Es gilt $\#(\lambda(\mathbb{R}) \cap g) > 1$.

Definition 4.17. Eine Gerade $g \in \mathrm{R}^2$ heisst *rational*, wenn sie die äquivalenten Bedingungen (i)–(iv) aus Aufgabe 4.16 A) erfüllt.

Für später halten wir fest:

Satz 4.18. *Sei $n \in \mathbb{N}$, sei*

$$F(x,y,z) = \sum_{i,j \in \mathbb{N}_0 : i+j \leq n} a_{i,j} x^i y^j z^{n-i-j}$$

eine nichtausgeartete diphantische n-Form. Sei weiter

$$f = f(u,v) := F(u,v,1) = \sum_{i,j \in \mathbb{N}_0 : i+j \leq n} a_{i,j} u^i v^j,$$

und sei $P := (u_0, v_0) \in \mathbb{M}(f(u,v))$. Dann ist

$$\mathbb{T}_P(f(u,v)) := \mathbb{M}\big(\frac{\partial f}{\partial u}(u-u_0) + \frac{\partial f}{\partial v}(v-v_0)\big)$$

die Tangente zu $f(u,v)$ im Punkt P. Ist P ein rationaler Punkt (d.h. gilt $u_0, v_0 \in \mathbb{Q}$), so ist $\mathbb{T}_P(f(u,v))$ eine rationale Gerade.

Beweis. Die gegebene Beschreibung der Tangente ist eine Wiederholung der Definition 4.15, die ihrerseits motiviert war durch das, was Sie in Aufgabe 4.14 D)(b) bewiesen haben. Die Rationalitätsaussage über diese Tangente folgt leicht mit dem, was Sie in Aufgabe 4.8 D)(b) gezeigt haben. □

Fernpunkte

Ein letzter Begriff, den wir nun einführen wollen, ist der Begriff des Fernpunkts einer Kurve. Wir schicken den Begriff des Fernpunkts der affinen Ebene $\mathbb{R}^2$ und den Begriff der projektiven Ebene voraus, allerdings in einer eher heuristischen Weise.

Definition und Bemerkung 4.19. A) Wir Betrachten die auf der *punktierten Ebene* $\mathbb{R}^2 \setminus \{(0,0)\}$ durch

$$(a,b) \approx (a',b') \Leftrightarrow \exists x \in \mathbb{R} \setminus \{0\} : a' = xa \wedge b' = xb$$

definierte Äquivalenzrelation. Die Äquivalenzklasse des Punktes $(a,b) \in \mathbb{R}^2 \setminus \{(0,0)\}$ bezeichnen wir mit $(a:b)$ und bilden die *(reelle) projektive Gerade*

$$\mathbb{P}^1 := \{(a:b) \mid (a,b) \in \mathbb{R}^2 \setminus \{(0,0)\}\}.$$

Die Klassen $(a:b) \in \mathbb{P}^1$ nennen wir *Punkte der projektiven Geraden* $\mathbb{P}^1$ und die Zahlen a und b nennen wir die *homogenen Koordinaten* des Punktes $(a:b)$. Die beiden homogenen Koordinaten eines Punktes sind natürlich nur bis auf ein gemeinsames Vielfaches bestimmt.
Ist $(a:b) \in \mathbb{P}^1$, so betrachten wir die durch den Ursprung $(0,0)$ und den Punkt (a,b) verlaufende Gerade

$$g_{(a:b)} \subset \mathbb{R}^2.$$

Die Zuordnung $(a:b) \mapsto g_{(a:b)}$ definiert so eine Bijektion zwischen der projektiven Geraden $\mathbb{P}^1$ und der Menge aller der durch den Ursprung laufenden Geraden in $\mathbb{R}^2$. Wir werden ab jetzt vermöge dieser Bijektion den Punkt $(a:b) \in \mathbb{P}^1$ auch mit der durch den Ursprung verlaufenden Geraden $g_{(a:b)}$ identifizieren.
Wir sagen der Fernpunkt $P = (a:b) \in \mathbb{P}^1$ sei *rational*, wenn die Gerade $g_{(a:b)}$ rational ist, d. h. wenn wir schreiben können

$$P = (a:b) \text{ mit } a,b \in \mathbb{Q}.$$

Die Menge der rationalen Fernpunkte, d. h. die Menge der rationalen Punkte von $\mathbb{P}^1$ nennen wir die *rationale projektive Gerade* und bezeichnen diese mit $\mathbb{P}^1_{\mathbb{Q}}$, also:

$$\mathbb{P}^1_{\mathbb{Q}} := \{(a:b) \mid (a,b) \in \mathbb{Q}^2 \setminus \{(0,0)\}\}.$$

B) Wir wollen nun die projektive Gerade $\mathbb{P}^1$ als *Ferngerade* unserer affinen Ebene $\mathbb{R}^2$ auffassen. Wir betrachten dazu die disjunkte Vereinigung

$$\mathbb{P}^2 := \mathbb{R}^2 \dot\cup \mathbb{P}^1,$$

die sogenannte *(reelle) projektive Ebene*. Ist $g \subset \mathbb{R}^2$ eine Gerade, so fassen wir die zu g parallele Gerade g' durch den Ursprung als Punkt in $\mathbb{P}^1$ auf und sagen

$$\infty_g := g' \in \mathbb{P}^1$$

sei der *Fernpunkt der Geraden* g. Ist

$$\lambda : \mathbb{R} \longrightarrow g, \quad t \mapsto \lambda(t) := (at + u_0, bt + v_0)$$

eine lineare Parametrisierung von g, können wir also auch schreiben:

$$\infty_g = (a : b)$$

Wir können nun den Ferpunkt ∞_g der Geraden g noch zu g hinzunehmen und schreiben

$$\overline{g} := g \dot{\cup} \{\infty_g\}.$$

Die Menge aller rationalen Punkte der projektiven Ebene nennen wir die *rationale projektive Ebene* und bezeichnen diese mit $\mathbb{P}^2_{\mathbb{Q}}$, also:

$$\mathbb{P}^2_{\mathbb{Q}} := \mathbb{Q}^2 \dot{\cup} \mathbb{P}^1_{\mathbb{Q}}.$$

C) Die reelle projektive Ebene $\mathbb{P}^2$ kann man aus der *rellen affinen Ebene* $\mathbb{R}^2$ so gewinnen, dass man für jede Gerade $g \subset \mathbb{R}^2$ die beiden gegenüberliegenden "Enden von g im Unendlichen" durch biegen von g im einzigem Fernpunkt ∞_g verklebt. Topolgisch gesehen kann man also ein Quadrat in der Ebene hernehmen, dessen Randpunkte als "unendlich ferne Punkte der Ebene" betrachten und je zwei "gegenüberliegende" dieser Randpunkte identifizieren. Wir können auch sagen, dass wir jeweils gegenüberliegende Seiten eines Quadrates verkleben, wobei wir vor dem Verkleben jeweils eine der beiden Seiten um 180^o drehen. Diese Verklebungsaufgabe lässt sich allerdings im dreidimensionalen Raum nur noch durchführen, wenn man eine *Selbstdurchdringung* der entstehenden *geschlossenen Fläche* in Kauf nimmt. Was wir so im dreidimensionalen Raum erhalten ist lediglich ein sogenanntes *Modell* der projektiven Ebene.
Die nachfolgende Abbildung soll den eben beschriebenen Deformations- und Verklebungsprozess für ein Quadrat beschrieben, der eine solche *Modellfläche* der projektiven Ebene liefert. Der Prozess wird in fünf Zwischenschritten dargestellt. Auffällig ist, dass beim vierten Schritt eine Schwierigkeit auftaucht: Die Notwendigkeit einer Selbstdurchdringung wirft ihren Schatten voraus. Der Prozess wird aber unbesehen davon zu Ende gefühert und die Selbstdurchdringung in Kauf genommen. Die geschlossene Fläche, die bei diesem Prozess entsteht, heisst das *Kreuzhaubenmodell* der projektiven Ebene. Deutlich tritt auf diesem Modell die Selbstdurchdringung zutage. Der Name dieses Modells soll durch die Abbildung ebenfalls gerechtfertigt werden. Schliesslich kann man an diesem Modell auch erkennen, dass die projektive Ebene *nicht orientierbar* ist, denn auf Kreuz dem Kreuzhaubenmodell tritt ein *Möbiusband* auf, wie in die Abbildung ebenfalls zeigt.

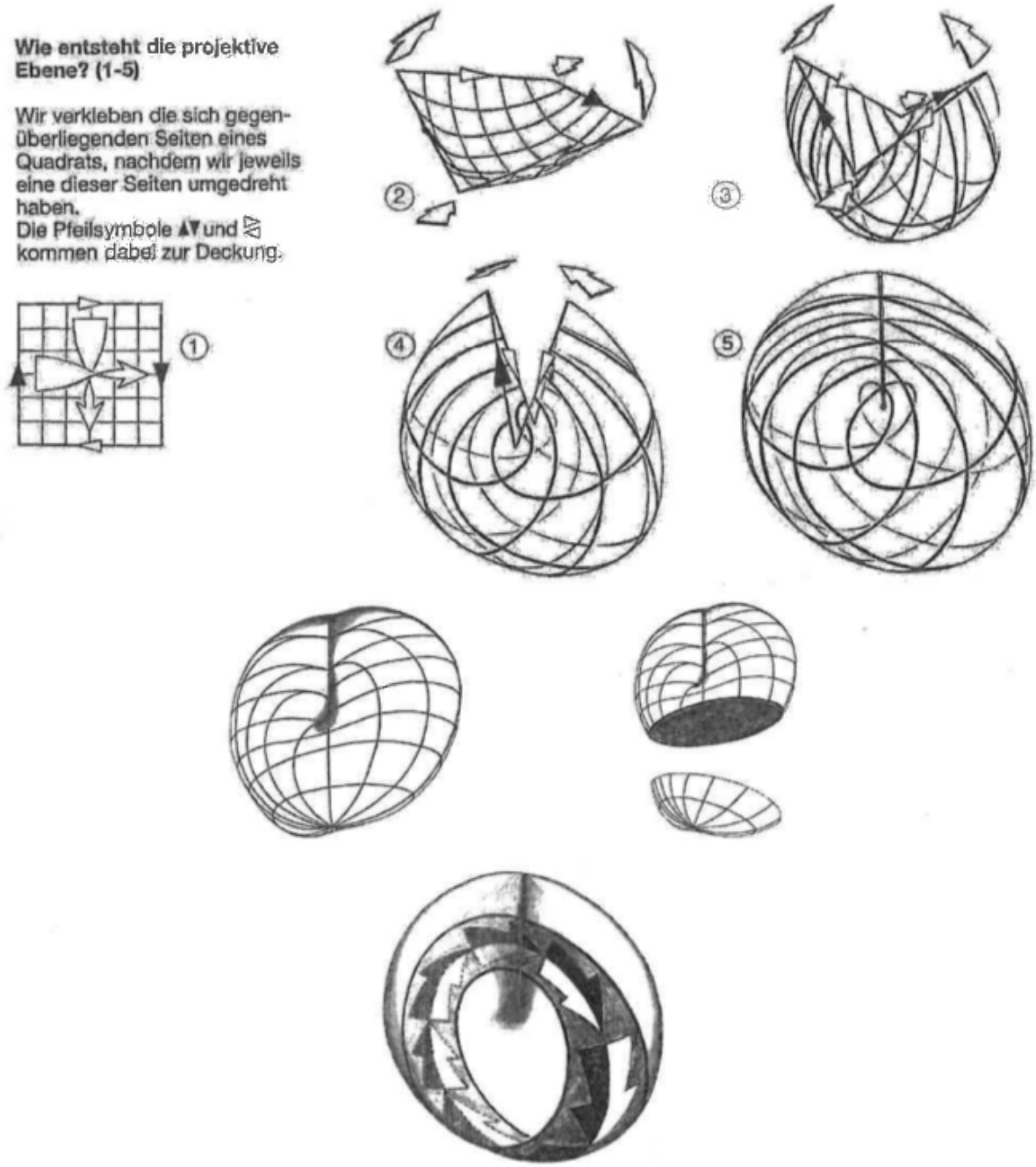


Abbildung 4.1: Kreuzhaubenmodell der projektiven Ebene

D) Sei nun $f(u,v) \in \mathbb{K}[u,v] \setminus \{0\}$. Wir sagen, $(a:b) \in \mathbb{P}^1$ sei ein *Fernpunkt von* $f(u,v)$, wenn die Gerade $g_{(a:b)}$ bezüglich $f(u,v)$ kritisch ist. Offenbar sind dann folgende Aussagen gleichbedeutend:

(i) $(a:b)$ ist ein Fernpunkt von $f(u,v)$;

(ii) $\mathbb{M}(bu-av) \subset \mathbb{M}\big(\mathrm{LF}(f(u,v))\big)$;

(iii) $bu-av$ teilt die Leitform $\mathrm{LF}(f(u,v))$ von $f(u,v)$.

Insbesondere können wir vermöge Aufgabe 4.14 A) sagen:

$$f(u,v) \text{ besitzt höchstens } \mathrm{Grad}(f(u,v)) \text{ verschiedene Fernpunkte .}$$

Wir führen die folgende Schreibweise ein:

$$\overline{\mathbb{M}}(f(u,v)) := \mathbb{M}(f(u,v)) \dot{\cup} \{(a:b) \in \mathbb{P}^1 \mid (a:b) \text{ ist Fernpunkt von } f(u,v)\}.$$

Dann können wir auch sagen:

$$\#\big(\overline{\mathbb{M}}(f(u,v)) \setminus \mathbb{M}(f(u,v))\big) \leq \mathrm{Grad}(f(u,v)).$$

D) Wir wollen nun das Konzept der Schnittvielfachheit erweitern. Sei $f(u,v) \in \mathbb{R}[u,v]$ und sei $g \subset \mathbb{R}^2$ eine Gerade. Sei $P \in \overline{g}$. Dann definieren wir die *Schnittvielfachheit von* $\overline{g}$ *mit* $f(u,v)$ *im Punkt* P durch

$$\mu_P(\overline{g}, f(u,v)) := \begin{cases} \mu_P(g, f(u,v)), & \text{falls } P \in g, \\ \mu_\infty(g, f(u,v)), & \text{falls } P = \infty_g. \end{cases}$$

Nach Definition und Bemerkung 4.13 E) gilt insbesondere

$$\sum_{P \in \overline{g}} \mu_P(\overline{g}, f(u,v)) \leq \mathrm{Grad}(f(u,v)).$$

E) Einen Fernpunkt $(a:b)$ von $f(u,v)$ nennen wir *rational*, wenn die Gerade $g_{(a:b)}$ rational ist, d.h. wenn $(a:b) \in \mathbb{P}^1_{\mathbb{Q}}$.

Schliesslich wollen wir das folgende Resultat festhalten:

Satz 4.20. *Sei* $n \in \mathbb{N}$ *mit* $n > 2$, *sei*

$$F(x,y,z) = \sum_{i,j \in \mathbb{N}_0 : i+j \leq n} a_{i,j} x^i y^j z^{n-i-j}$$

eine nichtausgeartete diphantische n-Form. Sei weiter

$$f = f(u,v) := F(u,v,1) = \sum_{i,j\in\mathbb{N}_0: i+j\leq n} a_{i,j}u^i v^j,$$

Sei weiter $g \subset \mathrm{R}^2$ *eine Gerade und sei*

$$\mathcal{P} \subset \overline{g} \cap \overline{\mathbb{M}}(f(u,v)) \text{ so, dass } \sum_{P\in\mathcal{P}} \mu_P\big(\overline{g}, f(u,v)\big) = n-1.$$

Dann gelten folgende Aussagen:

(a) *Es gibt genau einen Punkt* $Q \in \mathbb{P}^1 \setminus \mathcal{P}$ *so, dass* $\mathcal{P} \cup \{Q\} = \overline{g} \cap \overline{\mathbb{M}}(f(u,v))$.

(b) *Ist* $\mathcal{P} \subset \mathbb{P}^2_{\mathbb{Q}}$ *und gilt* $\mu_{\infty_g}(\overline{g}, f(u,v)) \neq n-1$, *so gilt auch* $Q \in \mathbb{P}^2_{\mathbb{Q}}$ *und die Gerade* g *ist rational.*

Beweis. Wir wählen eine lineare Parametrisierung von g:

$$\lambda : \mathbb{R} \longrightarrow g, \text{ mit } t \mapsto \lambda(t) = (l(t), h(t)), \text{ wobei}$$

$$l(t) = at + u_0, h(t) = bt + v_0 \in \mathbb{R}[t] \text{ so, dass } \max\{\mathrm{Grad}(l(t)), \mathrm{Grad}(h(t))\} = 1.$$

Weiter betrachten wir das Polynom

$$k(t) := f(\lambda(t)) = f(l(t), h(t)) = f(at + u_0, bt + v_0) \in \mathbb{R}[t].$$

Dann gilt nach Definition und Bemerkung 4.13 C), Satz 4.11 und Definition und Bemerkung 4.19 D) die Beziehung

$$\mathrm{Grad}(k(t)) = \mathrm{Grad}(f(u,v)) - \mu_\infty(g, f(u,v)) = n - \mu_{\infty_g}(\overline{g}, f(u,v)).$$

(a): Nehmen wir zuerst an, es sei $\mathcal{P} \subset g$. Dann folgt aus der in Definition und Bemerkung 4.19 D) gegebenen Ungleichung, dass

$$\mu_{\infty_g}(\overline{g}, f(u,v)) \leq 1.$$

Ist $\mu_{\infty_g}(\overline{g}, f(u,v)) = 1$, so können wir $Q = \infty_g$ wählen.
Sei also $\mu_{\infty_g}(\overline{g}, f(u,v)) = 0$. Dann ist $\mathrm{Grad}(k(t)) = n$. Setzen wir $Z := \lambda^{-1}(\mathcal{P})(\subset \mathbb{R})$, so gilt gemäss Definition und Bemerkung 4.13 A), dass $Z \subset \mathrm{Z}_{\mathbb{R}}(k(t))$ und

$$\sum_{z\in Z} \mu_z(k(t)) = \sum_{P\in\mathcal{P}} \mu_P(g, f(u,v)) = \sum_{P\in\mathcal{P}} \mu_P(\overline{g}, f(u,v)) = n-1.$$

Nun wenden wir Satz 4.6 auf das Polynom $k(t) \in \mathbb{R}[t]$ und finden ein $z' \in \mathbb{R} \setminus Z$ mit $Z \cup \{z'\} = \mathrm{Z}_{\mathbb{R}}(k(t))$ und $\mu_{z'}(k(t)) = 1$. Nun können wir gemäss Definition und Bemerkung 4.13 A) einfach $Q := \lambda(z')$ setzen.

Es bleibt der Fall zu behandeln, in dem $\infty_g \in \mathcal{P}$. Wir setzen $Z := \lambda^{-1}(\mathcal{P} \setminus \infty_g)$. gemäss Definition und Bemerkung 4.13 A) folgt nun

$$\begin{aligned}\sum_{z\in Z} \mu_z(k(t)) &= \sum_{P\in\mathcal{P}\setminus\{\infty_g\}} \mu_P(g, f(u,v)) = \sum_{P\in\mathcal{P}\setminus\{\infty_g\}} \mu_P(\overline{g}, f(u,v)) = \\ &= \big(\sum_{P\in\mathcal{P}} \mu_P(\overline{g}, f(u,v))\big) - \mu_{\infty_g}(\overline{g}, f(u,v)) = \\ &= n - 1 - \big(n - \mathrm{Grad}(k(t))\big) = \mathrm{Grad}(k(t)) - 1.\end{aligned}$$

Wieder nach Satz 4.6 – angewandt auf das Polynom $k(t)$ – finden wir ein $z' \in \mathbb{R} \setminus Z$ so, dass $\mathrm{Z}_{\mathbb{R}}(k(t)) = Z \cup \{z'\}$ und $\mu_{z'}(k(t)) = 1$. Wieder genügt es gemäss Definition und Bemerkung 4.13 A) einfach $Q = \lambda(z')$ zu setzen.

(b): Sei $\mathcal{P} \subset \mathbb{P}^2_{\mathbb{Q}}$. Nehmen wir zunächst an, es sei

$$\sum_{P\in\mathcal{P}} \mu_P\big(g, f(u,v)\big) > 1.$$

Dann ist g dann entweder Tangente zu f in einem der Punkte $P \in \mathcal{P} \cap \mathbb{Q}^2$ oder enthält zwei verschiedene rationale Punkte $P, P' \in \mathcal{P} \cap \mathbb{Q}^2$. In jedem Fall ist also g eine rationale Gerade (s. Satz 4.18). Damit können wir annehmen, es seien $t(t), h(t) \in \mathbb{Q}[t]$. Dann ist aber $k(t) \in \mathbb{Q}[t]$. Nun können wir den Beweis von Aussage (a) nochmals durchgehen, aber dabei überall $\mathbb{R}$ durch $\mathbb{Q}$ ersetzen, und erhalten so unsere Behauptung.
Nehmen wir als nächstes an, es sei

$$\sum_{P\in\mathcal{P}} \mu_P\big(g, f(u,v)\big) = 1.$$

Dann ist $\infty_g \in \mathcal{P} \subset \mathbb{P}^2_{\mathbb{Q}}$ und g enthält einen weiteren Punkt $P \in \mathcal{P} \cap \mathbb{Q}^2$. Damit ist aber die Gerade g wieder rational, und wir können schliessen wie vorhin.
Sei schliesslich $\sum_{P\in\mathcal{P}} \mu_P\big(g, f(u,v)\big) = 0$. Dann ist $\mathcal{P} = \{\infty_g\}$ und

$$\mu_\infty(g, f(u,v)) = \mu_{\infty_g}(\overline{g}, f(u,g)) = n - 1,$$

was unserer Voraussetzung widerspricht. □

Elliptische Kurven

Bemerkung und Definition 4.21. A) Sei

$$\begin{aligned}F(x,y,x) &= \sum_{i,j\in\mathbb{N}_0 : i+j\le 3} a_{i,j} x^i y^j z^{3-i-j} = \\ &= a_{3,0}x^3 + a_{2,1}x^2y + a_{2,0}x^2z + a_{1,2}xy^2 + a_{1,1}xyz + \\ &+ a_{1,0}xz^2 + a_{0,3}y^3 + a_{0,2}y^2z + a_{0,1}yz^2 + a_{0,0}z^3\end{aligned}$$

eine *nichtausgeartete diophantische Kubik*. Ist $\mathbb{L}(F(x,y,z)) \neq \{(0,0,0)\}$, d.h. gibt es ein Tripel $(x_0,y_0,z_0) \in \mathbb{Z}^3 \setminus \{(0,0,0)\}$ mit $f(x_0,y_0,z_0) = 0$ (s. Bemerkung und Definition 4.2 A)(a)), so sagt man die nichtausgeartete diophantische 3-Form $F(x,y,z)$ *definiere eine elliptische Kurve*. Kürzer sagen wir in dieser Situation einfach auch $F(x,y,z)$ *sei eine elliptische Kurve*.

B) Sei $F(x,y,z)$ eine elliptische Kurve. Dann kann man $F(x,y,z)$ durch eine lineare Koordinatentransformation immer auf die spezielle Form bringen, bei welcher

(1) $a_{3,0} = -1, a_{0,2} = 1$,

(2) $a_{2,1} = a_{2,0} = a_{1,2} = a_{1,1} = a_{0,1} = a_{0,3} = 0$,

(3) $a_{1,0} = -a \in \mathbb{Q}$ und $a_{0,0} = b \in \mathbb{Q}$.

(4) $27b^2 + 4a^3 \neq 0$.

Man kann dann also insbesondere schreiben

$$F(x,y,z) = y^2z - X^3 - axz^2 + bz^3 \text{ mit } a,b \in \mathbb{Q} \text{ und } 27b^2 + 4a^3 \neq 0.$$

Die Koeffizienten sind dabei eindeutig durch $F(x,y,z)$ festgelegt. Man nennt diese Gestalt der elliptischen Kurve $F(x,y,z)$ die *(Weierstrass'sche) Normalform*.

C) Sei nun

$$F(x,y,z) = y^2z - x^3 - axz^2 + bz^3 \text{ mit } a,b \in \mathbb{Q} \text{ und } 27b^2 + 4a^3 \neq 0.$$

eine elliptische Kurve in Normalform. Die sogenannte *affine Normalform* der elliptischen Kurve $F(x,y,z)$ ist dann definiert als das Polynom

$$f(u,v) := F(u,v,1) = v^2 - u^3 - au + b, \text{ wobei wieder } a,b \in \mathbb{Q} \text{ und } 27b^2 + 4a^3 \neq 0.$$

Die Theorie der elliptischen Kurven untersucht die Lösungsmenge $\mathbb{L}(F(x,y,z))$ der homogenen diophantischen Gleichung $F(x,y,z) = 0$ oder, was gleichbedeutend ist, die Menge

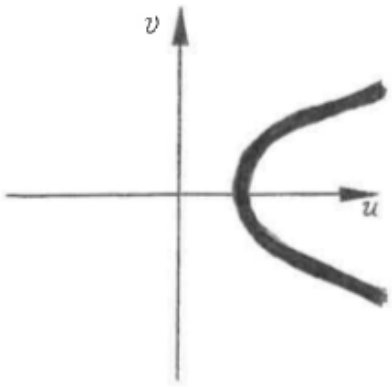
$$\mathbb{E}(f(u,v)) = \mathbb{P}^2_{\mathbb{Q}} \cap \overline{\mathbb{M}}(f(u,v))$$

der rationalen Punkte auf der Kurve $\overline{\mathbb{M}}(f(u,v)) \subset \mathbb{P}^2$.

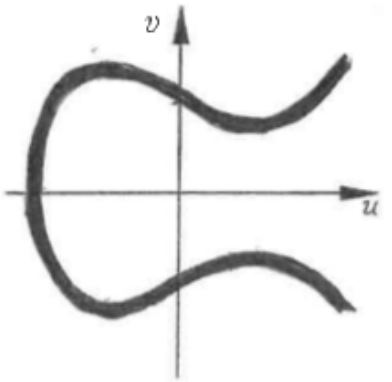
Die Bedeutung der in Bemerkung und Defnition 4.21 B)(4) genannten Nebenbedingung $27b^2 + 4a^3 \neq 0$ wird in der nachfolgenden Übungsaufgabe klar gestellt. Die nächste Abbildung illustriert an einigen Beispielen, wie die Gestalt der Kurve

$$\mathbb{M}(f(u,v)) = \mathbb{M}(v^2 - u^3 - au + b)$$

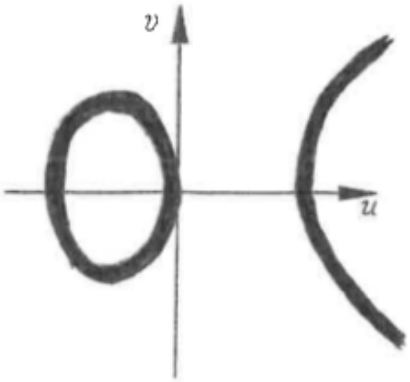
von den Koeffizienten a und b abhängt.



$\mathbb{M}(f(u,v)) = \mathbb{M}(v^2 - u^3 + 1)$



$\mathbb{M}(f(u,v)) = \mathbb{M}(v^2 - u^3 + 3u - 3)$



$\mathbb{M}(f(u,v)) = \mathbb{M}(v^2 - u^3 + 4u)$

Abbildung 4.2: Beispiele elliptischer Kurven

Aufgaben 4.22. A) Sei $f(u,v) := F(u,v,1) = v^2 - u^3 - au + b, (a, b \in \mathbb{Q})$ eine elliptische Kurve in affiner Normalform. Zeigen Sie, dass die Bedingung $27b^2 + 4a^3 \neq 0$ notwendig und hinreichend dafür ist, dass $F(x,y,z)$ nicht ausgeartet ist.

B) Es gelten weiterhin die Bezeichnungen von Teil A). Zeigen Sie, dass

$$\infty := \infty_{f(u,v)} = (0:1)$$

der einzige Fernpunkt von $f(u,v)$ ist. Zeigen Sie auch, dass $\infty \in \mathbb{P}^1_{\mathbb{Q}}$ und dass

$$\mu_\infty(\overline{g}, f(u,v)) = 1 \text{ für jede Gerade } g, \text{ die parallel ist zur } v - \text{Achse} \mathbb{M}(u).$$

C) Es gelten nach wie vor die obigen Bezeichnungen. Seien $P, Q \in \overline{\mathbb{M}}(f(u,v))$ mit $(P,Q) \neq (\infty, \infty)$. Sei $\langle P, Q\rangle \subset \mathbb{R}^2$ die wie folgt definierte Gerade:

$$\langle P,Q\rangle := \begin{cases} \text{Gerade durch } P \text{ und } Q, & \text{falls } P,Q \neq \infty \text{ und } P \neq Q; \\ \text{Tangente zu } f(u,v) \text{ in } P, & \text{falls } P = Q \neq \infty; \\ \text{Gerade durch } P \text{ und parallel zu } \mathbb{M}(u), & \text{falls } P \neq Q = \infty; \\ \text{Gerade durch } Q \text{ und parallel zu } \mathbb{M}(u), & \text{falls } Q \neq P = \infty. \end{cases}$$

Zeigen Sie, dass $\langle P,Q\rangle = \langle Q,P\rangle$. Zeigen Sie, dass

(a) $2 \leq \kappa(P,Q) := \sum_{S \in \{P,Q\}} \mu_S(\overline{g}, f(u,v)) \leq 3$.

Zeigen Sie mit Hilfe von Satz 4.20 (a):

[(b) Ist $\kappa(P,Q) = 2$, so gibt es einen eindeutig bestimmten Punkt $V_{P,Q} \in \mathbb{P}^2 \setminus \{P,Q\}$ so, dass

$$\overline{\langle P,Q\rangle} \cap \overline{\mathbb{M}}(f(u,v)) = \{P, Q, V_{P,Q}\}$$

Schliessen Sie mit Aufgabe B) und Satz 4.20 (b), dass folgendes gilt:

(c) Ist $\kappa(P,Q) = 2$ und gilt $P, Q \in \mathbb{P}^2_{\mathbb{Q}}$, so gilt auch $V_{P,Q} \in \mathbb{P}^2_{\mathbb{Q}}$.

D) Es gelten die obigen Bezeichnungen. Zeigen Sie:

(a) $\mathbb{M}(f(u,v))$ ist spiegelungssymetrisch bezüglich der u-Achse, d.h. für alle $(u_0, v_0) \in \mathbb{R}^2$ gilt:

$$(u_0, v_0) \in \mathbb{M}(f(u,v)) \Leftrightarrow (u_0, -v_0) \in \mathbb{M}(f(u,v)).$$

(b) Ist $P = (u_0, v_0) \in \mathbb{M}(f(u,v))$ mit $v_0 \neq 0$ so gilt:

$$\kappa(P, \infty) = 2 \text{ und } (u_0, -v_0) = V_{P,\infty}.$$

Definition und Bemerkung 4.23. A) Sei

$$f(u,v) := F(u,v,1) = v^2 - u^3 - au + b, (a, b \in \mathbb{Q}, 27b^2 + 4a^3 \neq 0)$$

eine elliptische Kurve in affiner Normalform. Es gelten alle Bezeichnungen von Aufgabe 4.22 C). Ist $(P,Q) \in \overline{\mathbb{M}}(f(u,v))^2 \setminus \{(\infty,\infty)\}$ mit $\kappa(P,Q) = 2$, so nennen wir die Gerade $\langle P,Q\rangle$ die *Verbindungsgerade* von P und Q, und den Punkt $V_{P,Q}$ den *Verbindungspunkt* von P und Q. Der Verbindungspunkt $V_{P,Q}$ ist charaktersisiert durch die Eigenschaft

$$\overline{\langle P,Q\rangle} \cap \overline{\mathbb{M}}(f(u,v)) = \{P, Q, V_{P,Q}\}.$$

Es handelt sich also um den Punkt, den man erhält, wenn man P und Q durch die (im Unendlichen durch ihren Fernpunkt ergänzten) Gerade $\overline{\langle P,Q\rangle}$ verbindet und dann den "dritten" Schnittpunkt dieser Geraden mit der Kurve $\overline{\mathbb{M}}(f(u,v)) \subset \mathbb{P}^2$ bildet.

B) Es gelten die obigen Bezeichnungen. Durch die Spiegelung an der u-Achse können wir auf $\overline{\mathbb{M}}(f(u,v))$ wie folgt eine *Involution* definieren:

$$\bullet^{-1} : \overline{\mathbb{M}}(f(u,v)) \longrightarrow \overline{\mathbb{M}}(f(u,v)), \quad P \mapsto P^{-1}, \text{ wobei}$$

$$P^{-1} := \begin{cases} (u_0, -v_0), & \text{falls } P = (u_0, v_0) \neq \infty \text{ und } v_0 \neq 0; \\ P, & \text{falls } P = (u_0, 0) \neq \infty \\ \infty, & \text{falls } P = \infty. \end{cases}$$

Nach Aufgabe 4.22 D)(b) knnen wir auch schreiben:

$$P^{-1} = \begin{cases} V_{P,\infty}, & \text{falls } P = (u_0, v_0) \neq \infty \text{ mit } v_0 \neq 0; \\ P, & \text{sonst .} \end{cases}$$

C) Es gelten immer noch die obigen Bezeichnungen. Wir können auf $\overline{\mathbb{M}}(f(u,v)$ wie folgt eine *binäre Operation* $*$ definieren:

$$* : \overline{\mathbb{M}}(f(u,v))^2 \longrightarrow \overline{\mathbb{M}}(f(u,v)), \text{ wobei}$$

$$P * Q := \begin{cases} V_{V_{P,Q},\infty}, & \text{falls } (P,Q) \neq (\infty,\infty), \kappa(P,Q) = 2 \text{ und } V_{P,Q} \neq \infty \\ \infty, & \text{sonst .} \end{cases}$$

Mit Hilfe der in Teil B) eingeführten Involution $\bullet^{-1}$ können wir auch schreiben:

$$P * Q = \begin{cases} (V_{P,Q})^{-1}, & \text{falls } (P,Q) \neq (\infty,\infty), \kappa(P,Q) = 2 \text{ und } V_{P,Q} \neq \infty \\ \infty, & \text{sonst .} \end{cases}$$

D) Man kann nun leicht nachrechnen, dass die eben eingeführte Operation $*$ *kommutativ* ist, das *Neutralelement* ∞ hat, und dass die Involution $\bullet^{-1}$ der *Inversion* von $*$ entspricht, also:

(a) $P * Q = Q * P$ für alle $P, Q \in \overline{\mathbb{M}}(f(u,v))$;

(b) $\infty * P = P * \infty$ für alle $P \in \overline{\mathbb{M}}(f(u,v))$;

(c) $P * P^{-1} = P^{-1} * P = \infty$ für alle $P \in \overline{\mathbb{M}}(f(u,v))$.

Man kann aber auch beweisen, dass die Operation $*$ *assoziativ* ist:

(d) $P * (Q * S) = (P * Q) * S$ für alle $P, Q, S \in \overline{\mathbb{M}}(f(u,v))$.

Damit können wir schliesslich sagen:

$$\overline{\mathbb{M}}(f(u,v)) = \big(\overline{\mathbb{M}}(f(u,v)), *, \infty\big) \text{ ist eine abelsche Gruppe.}$$

E) Es gelten weiterhin die obigen Bezeichnungen. Mit Hilfe von Aufgaben 4.22 B) und C)(c) folgt nun leicht, dass die Menge

$$\mathbb{E}(f(u,v)) := \mathbb{P}^2_{\mathbb{Q}} \cap \overline{\mathbb{M}}(f(u,v))$$

den Punkt ∞ enthält und *abgeschlossen* ist bezüglich der Operation $*$ und natürlich auch bezüglich der Involution $\bullet^{-1}$:

(a) $\infty \in \mathbb{E}(f(u,v))$;

(b) $P, Q \in \mathbb{E}(f(u,v)) \Rightarrow P * Q \in \mathbb{E}(f(u,v))$;

(c) $P \in \mathbb{E}(f(u,v)) \Rightarrow P^{-1} \in \mathbb{E}(f(u,v))$.

Folglich können wir nun auch sagen:

$$\mathbb{E}(f(u,v)) = \big(\mathbb{E}(f(u,v)), *, \infty\big) \text{ ist eine Untergruppe von } \overline{\mathbb{M}}(f(u,v)).$$

Auf der nächsten Seite ist die oben eingeführte Operation $*$ geometrisch dargestellt.

Aufgaben 4.24. A) Es gelten die obigen Bezeichnungen. Beweisen Sie, dass $(P^{-1})^{-1} = P$ für alle $P \in \overline{\mathbb{M}}(f(u,v))$.

B) Beweisen Sie die Aussagen (a),(b),(c) aus Definition und Bemerkung 4.23 D) und die Aussagen (a),(b),(c) aus Definition und Bemerkung 4.23 E).

C) Zeigen Sie, dass die Punkte $P, Q, (P * Q)^{-1}$ für alle $P, Q \in \overline{\mathbb{M}}(f(u,v))$ kollinear sind.

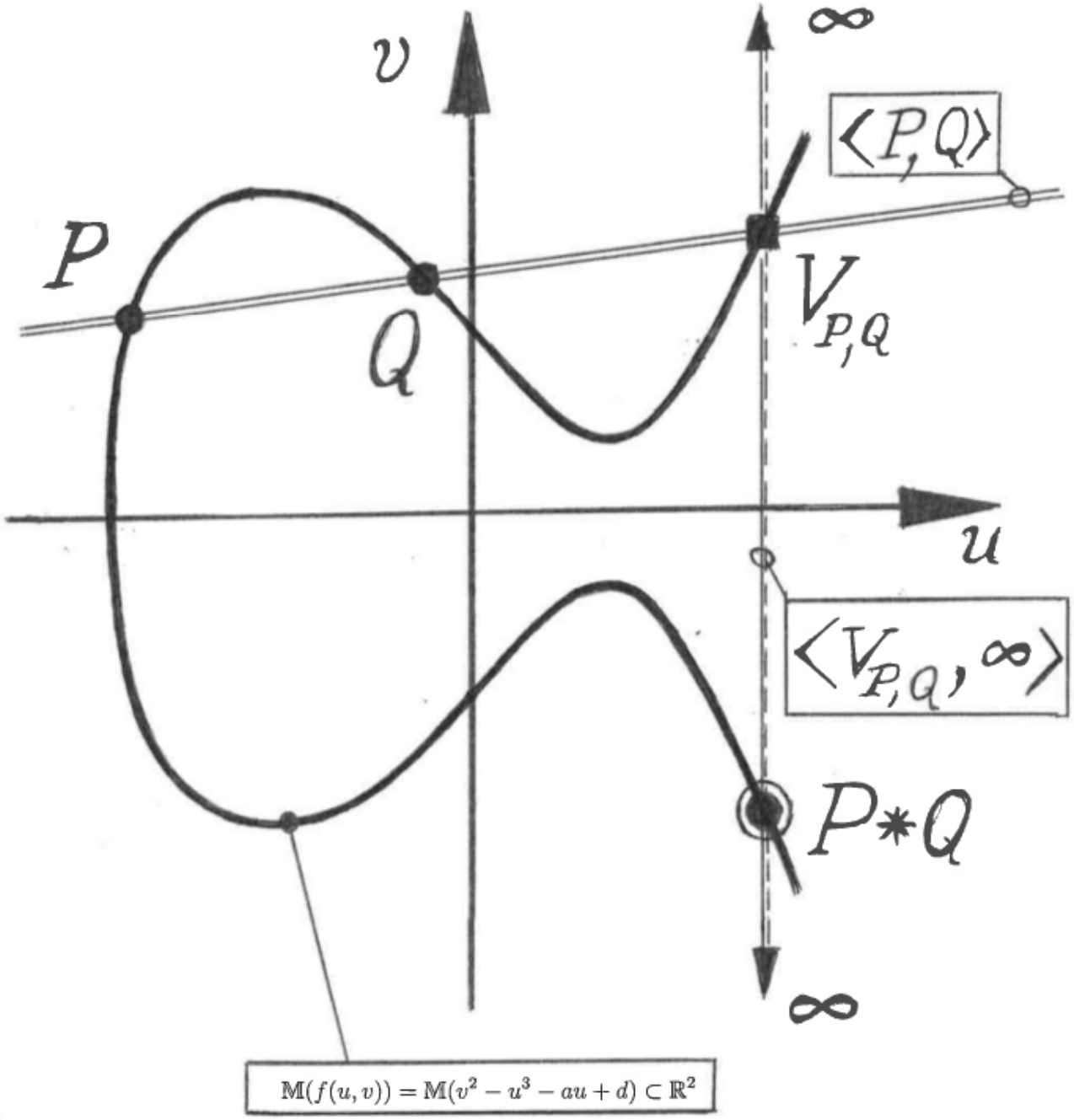


Abbildung 4.3: Gruppenoperation der elliptischen Kurven

Nun formulieren wir den zweifellos wichtigste Satz über die elliptischen Kurven, den wir natürlich hier nicht beweisen werden:

Satz 4.25. *(Mordell, 1922) Sei*

$$f(u,v) := F(u,v,1) = v^2 - u^3 - au + b, (a, b \in \mathbb{Q}, 27b^2 + 4a^3 \neq 0)$$

eine elliptische Kurve in affiner Normalform. Dann ist die abelsche Gruppe

$$\overline{\mathbb{M}}(f(u,v)) \cap \mathbb{P}^2_{\mathbb{Q}} =: \mathbb{E}(f(u,v)) = \big(\mathbb{E}(f(u,v)), *, \infty\big)$$

endlich erzeugt.

Korollar 4.26. *Es gelten die Bezeichnungen und Voraussetzungen von Satz 4.25. Dann gibt es endlich viele Punkte $P_1, \ldots, P_r \in \mathbb{E}(f(u,v)) \setminus \{\infty\}$ derart, dass jeder weitere Punkt $P \in \mathbb{E}(f(u,v))$ durch endlich oft wiederholtes bilden von Verbindungspunkten und Spiegelungen an der u-Achse entseht.*

Bemerkung 4.27. A) Mit dem obigen Satz von Mordell tauchten – wie so oft, wenn in der Mathematik ein Resultat gefunden wird – neue Fragen auf. Eine endlich erzeugte abelsche Gruppe $G = (G, *, 0)$ ist nach den *Hauptsatz über abelsche Gruppen* immer isomorph zu einer direkten Summe von (additiven) Gruppen:

$$\mathbb{Z}^r \oplus T, \text{ mit } T = \oplus_{i=1}^s \mathbb{Z}/p_i^{n_i}\mathbb{Z},$$

mit eindeutig bestimmten Zahlen $r, s \in \mathbb{N}_0$, eindeutig bestimmten Primzahlen $p_1 \leq p_2 \leq \ldots \leq p_r$, und eindeutig bestimmten Zahlen $n_1, n_2, \ldots, n_r \in \mathbb{N}$. Die Zahl

$$r := \text{Rang}(G) \in \mathbb{N}_0$$

heisst dann der *Rang* von G. Die Folge

$$(p_i^{n_i})_{i=1}^s := \tau(G) \in \mathbb{N}^s$$

nennen wir die *Torsionscharakteristik* der Gruppe G. Durch die numerischen invarianten $\text{Rang}(G)$ und $\tau(G)$ ist die Gruppe G bis auf Isomorphie bestimmt. Deshalb ist es naheliegnd, dass man nach dem Beweis des Satzes von Mordell mit der Untersuchung der Invarianten

$$\text{Rang}(f(u,v)) := \text{Rang}\big(\mathbb{E}(f(u,v))\big) \text{ und } \tau(f(u,v)) := \tau\big(\mathbb{E}(f(u,v))\big),$$

begann, die wir auch als *Rang* respektive *Torsionscharakterstik* der elliptischen Kurve $f(u,v))$ bezeichnen.

B) Das *Torsionsproblem* für elliptische Kurven, d.h. die Bestimmung aller mglichen Torsionscharakteristiken $\tau(f(u,v))$ ist im Wesentlichen seit ca. 1980 gelöst. Allerdings scheint bis heute kein allgemeiner Algorithmus bekannt zu sein, der die Berechnung der Torsionscharaktersitik $\tau(f(u,v))$ aus den Koeffizienten a, b des kubischen Polynoms $f(u,v) = v^2 - u^3 - au + b$ erlaubt.
Wesentlich schwieriger als das Torsionsproblem präsentiert sich das *Rangproblem* für elliptische Kurven. So wird etwa vermutet, dass jede Zahl $r \in \mathbb{N}_0$ Rang einer elliptischen Kurve sein kann. Man ist allerdings noch weit davon entfernt, einen Beweis für diese Vermutung zu haben. Es ist nur für ca. 30 Zahlen $r \in \mathbb{N}_0$ bewiesen, dass es eine elliptische Kurve vom Rang r gibt. Noch weiter ist man davon entfernt, einen allgemeinen Algorithmus zur Bestimmung des Ranges $\mathrm{Rang}(f(u,v))$ der elliptischen Kurve aus den Koeffizienten a, b des Polynoms $f(u,v) = v^2 - u^3 - au + b$ zu kennen.
Das "Traumresultat" zu finden – ein Verfahren zur Bestimmung der in Korollar 4.26 genannten *erzeugenden Punkte* $P_1, \ldots, P_r$ für die elliptische Kurve $f(u,v)$ – liegt also noch in weitester Ferne.

C) Man kann auch "elliptische Kurven" $f(u,v) = v^2 - u^3 - au + b$ betrachten, deren Koeffizienten a, b in einem endlichen Körper $\mathbb{K}$ liegen – zum Beispiel in $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$, wo $p \in \mathbb{N}$ eine Primzahl ist. Auch diese elliptischen Kurven lassen sich in ähnlicher Weise zu (endlichen) abelschen Gruppen machen, wie wir dies vorhin getan haben. Solche elliptische Kurven spielen heute eine wichtige Rolle in der *Kryptographie*, der Lehre von der Verschlüsselung und Entschlüsselung von Zeichen- oder Ziffernfolgen.
Die meisten Anwendungen in diesem Gebiet beruhen darauf, dass das *diskrete Logarithmieren* in (endlichen) elliptischen Kurven algorithmisch sehr aufwändig ist im Vergleich zum Potenzieren. Anders gesagt:

- Ist P ein Punkt einer elliptischen Kurve $\mathbb{E}$ und ist $n \in \mathbb{N}$, so lässt sich der Punkt $Q := P * P * \cdots * P = P^{*n}$ "relativ schnell" berechenen.
- Andrerseits ist im Allgemeinen bei gegebenen $P, Q \in \mathbb{E}$ das Aufsuchen des *diskreten Logarithmus*
$$\log_P(Q) := \min\{n \in \mathbb{N} \mid P^{*n} = Q\}$$
von Q zur Basis P mit grossen Aufwand verbunden.
- Dasselbe gilt im Allgemeinen auch für das Dividieren durch natürliche Zahlen oder – gleichbedeutend – das Wurzelziehen in $\mathbb{E}$, d.h. für die Bestimmung von
$$Q^{\frac{*}{n}}, \text{ definiert durch } \left(Q^{\frac{*}{n}}\right)^{*n} = Q.$$

Elliptische Kurven und die Fermat-Vermutung

Bekanntlich haben Taylor und Wiles im Jahre 1995 gezeigt, dass die *Fermat-Vermutung* richtig ist (vgl. Kapitel 1):

Korollar 4.28. *(Taylor-Wiles, 1995) Sei $n \in \mathbb{N}$ mit $n > 2$. Seien $x, y, z \in \mathbb{N}$. Dann gilt*

$$x^n + y^n \neq z^n.$$

Bemerkung 4.29. Wie wir schon früher bemerkt haben, ist der obige Satz von Fermat als Vermutung ausgesprochen worden. Fast vier Jahrhunderte lang hat sich diese Vermutung mindestens im Allgemeinfall hartnäckig allen Beweisversuchen widersetzt. Andrerseits ist die Vermutung im Verlaufe der Zeit in vielen Spezialfällen bewiesen worden. Seit Fermat seine Vermutung äusserte erschien in der Tat ist eine unabsehbare Menge von Beiträgen zu dieser Frage. Wahrscheinlich war die Fermat-Vermutung sogar der "stärkste Motor" für die Entwicklung der Zahlentheorie, insbesondere der im 19. Jahrhundert entstandenen *algebraischen Zahlentheorie*.
Wir wollen hier eine Reduktion des Fermat-Problens nennen, die schon zu Beginn des 19. Jahrhunderts bekannt war:

- Gilt das Korollar 4.28 für alle primen Exponenten $p = n > 2$, so gilt er für alle ganzen Exponenten $n > 3$.

Interssant ist, dass der Beweis dieses Satzes sehr tiefe Resultate aus der Theorie der elliptischen Kurven benutzt. Wir wollen dazu einige Bemerkungen machen.

Bemerkung und Definition 4.30. A) Sei

$$\mathbb{H} := \{z = a + ib \in \mathbb{C} \mid \mathrm{im(z)} = \mathrm{b} > 0\}$$

die *komplexe obere Halbebene*. Eine *meromorphe Funktion*

$$f : \mathbb{H} \cdots \longrightarrow \mathbb{C}$$

ist eine holomorphe (d.h. im komplexen differenzierbare) Funktion

$$f : \mathbb{H} \setminus \mathrm{Pol}(f) \longrightarrow \mathbb{C}$$

so, dass die *Polmenge* $\mathrm{Pol}(f) \subset \mathbb{H}$ von f nur *isolierte Punkte* enthält. Dies heisst:

$$\text{Ist } z \in \mathrm{Pol}(f), \text{ so gibt es ein } \varepsilon > 0 \text{ so, dass } w \notin \mathrm{Pol}(f) \text{ für alle } w \in \mathbb{H} \text{ mit } |w - z| < \varepsilon.$$

B) Wir betrachten als erstes die *spezielle arithmetische Gruppe von Rang* 2, d.h. die Matrizengruppe

$$\mathrm{SL}_2(\mathbb{Z}) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \text{ mit } ad - cd = 1\}.$$

Sei $k \in \mathbb{N}_0$. Eine *Modulfunktion vom Gewicht k* ist eine meromorphe Funktion

$$m : \mathbb{H} \cdots \longrightarrow \mathbb{C}$$

mit den folgenden Eigenschaften:

(a) Für alle $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ und alle

$$z \in \mathbb{H} \setminus \mathrm{Pol}(m) \text{ mit } cd + d \neq 0 \text{ und } \frac{az+b}{cz+d} \in \mathbb{H} \setminus \mathrm{Pol}(m) \text{ gilt.}$$

$$m\big(\frac{az+b}{cz+d}\big) = (cz+d)^k m(x).$$

(b) Für alle $z \in \mathbb{H}$ mit $z, -z^{-1} \notin \mathrm{Pol}(m)$ gilt

$$m(-z^{-1}) = z^k m(z).$$

(c) Für alle $z \in \mathbb{H} \setminus \mathrm{Pol}(m)$ gilt:

$$z+1 \notin \mathrm{Pol}(m) \text{ und } m(z+1) = m(z).$$

Eine Schlüsselstellung im Beweis von Taylor-Wiles hat die folgende Vermutung

Vermutung 4.31. *(Taniyama-Shimura, 1955) Jede elliptische Kurve*

$$f(u,v) := F(u,v,1) = v^2 - u^3 - au + b, (a, b \in \mathbb{Q}, 27b^2 + 4a^3 \neq 0)$$

in affiner Normalform ist modular. Das heisst: Es gibt ein $k \in \mathbb{N}_0$ und zwei nichtkonstante Modulfunktionen

$$m_1, m_2 : \mathbb{H} \cdots \longrightarrow \mathbb{C} \text{ vom Gewicht } k \text{ so, dass}$$

$$f(m_1(z), m_2(z)) = m_1(z)^2 - m_2(z)^3 - am_2(z) + b = 0$$
$$\text{für alle } z \in \mathbb{H} \setminus \big(\mathrm{Pol}(m_1) \cup \mathrm{Pol}(m_2)\big).$$

Bemerkung und Definition 4.32. Sei $p > 2$ eine Primzahl und seien $x, y \in \mathbb{N}$. Wir setzen

$$\overline{u} := u + \frac{x^p - y^p}{3}$$

und betrachten das Polynom

$$\overline{f}(\overline{u}, v) = \overline{f}_{p,x,x}(\overline{u}, v) := v^2 - \overline{u}(\overline{u} - x^p)(\overline{u} + y^p) \in \mathbb{Q}[\overline{u}, v],$$

das wir die *Frey'sche Kubik* zum Tripel (p, x, z) nennen. Wir fassen dieses Polynom als Polynom in den Variablen u, v auf und schreiben entsprechend

$$\overline{f}_{p,x,y}(\overline{u}, v) =: f_{p,x,y}(u, v) = f(u, v) \in \mathbb{Q}[u, v].$$

Dann kann man zeigen, dass das Polynom $f(u, v)$ eine elliptische Kurve in affiner Normalform ist – die *Frey'sche elliptische Kurve* zum Tripel (p, x, y).

Aufgaben 4.33. Sei $p > 2$ eine Primzahl und seien $x, y \in \mathbb{N}$. Berechnen Sie das in Bemerkung und Definition 4.32 definierte Polynom $f_{p,x,y}(u, v) \in \mathbb{Q}[u, v]$ und zegen Sie, dass es sich um eine elliptische Kurve in affiner Normalform handelt.

Nun können wir das folgende Ergebnis festhalten:

Satz 4.34. *(vermutet 1985 von Frey, bewiesen 1986 von Ribet) Sei $p > 2$ eine Primzahl und seien $x, y \in \mathbb{N}$. Wenn es ein $z \in \mathbb{N}$ so gibt, dass*

$$x^p + y^p = z^p,$$

dann ist die Frey'sche elliptische Kurve $f_{p,x,y}(u, v)$ nicht modular.

Bemerkung 4.35. Seien $p > 2$ eine Primzahl und $x, y \in \mathbb{N}$ und sei $f_{p,x,y}(u, v)$ die Frey'sche elliptische Kurve zum Tripel (p, x, y). Diese elliptische Kurve hat dann eine Eigenschaft, die man *Semistabiltät* nennt. Wir definieren hier allerdings diesen Begriff – d. h. den Begriff der *semistabilen elliptischen Kurve* – nicht.

Nun können wir den eigentlichen Satz von Taylor und Wiles formulieren, aus dem dann Korollar 4.28 folgt.

Satz 4.36. *(Taylor-Wiles, 1995) Für semistabile elliptische Kurven gilt die Taniyama-Shimura-Vermutung.*

Aufgaben 4.37. Beweisen Sie das Korollar 4.28 aus Satz 4.36.

Diophantische Formen vom Grad > 3

Als krńenden Abschluss unseres Ausblickes wollen wir auf ein Resultat hinweisen, dass mehr als ein halbes Jahrhundert lang als die herausfordernste Vermutung der diophantischen Geometrie gegolten hat: die sogenanne *Mordell-Vermutung*.

Satz 4.38. *(vermutet 1922 von Mordell, bewiesen 1983 von Faltings) Sei $n \in \mathbb{N}$ mit $n > 3$, sei $F(x, y, z)$ eine nichtausgeartete diophantische n-Form und sei*

$$f(u, v) := F(u, v, 1)\big(\in \mathbb{Q}[u, v]\big).$$

Dann enthält $\mathbb{M}(f(u, v))$ nur endlich viele rationale Punkte, das heisst es gilt:

$$\#\big(\mathbb{Q}^2 \cap \mathbb{M}(f(u, v))\big) = \#\{(u_0, v_0) \in \mathbb{Q}^2 \mid f(u_0, v_0) = 0\}\big) < \infty.$$

Aufgaben 4.39. A) Es gelten die Bezeichnungen und Voraussetzungen von Satz 4.38. Zeigen Sie, dass

$$\#\big(\mathbb{P}^2_{\mathbb{Q}} \cap \overline{\mathbb{M}}(f(u, v))\big) < \infty.$$

Schliessen Sie daraus, dass in den Bezeichnungen von Definition 4.1 gilt

$$\#\big(\mathbb{L}(F(x,y,z)) < \infty.$$

B) Was wir insgesamt in den Kapiteln 3 und 4 gelernt haben zeigt, dass bei zunehmendem Grad n der nichtausgearteten diophantischen n-Form die Lösungsmenge $\mathbb{L}(F(x,y,x))$ der nichtausgearteten diophantischen n-Formen "immer kleiner wird". Präzisieren sie diese Aussage aufgrund der in den genannten Kapiteln bewiesenen Resultaten.

C) Es gelten immer noch die obigen Bezeichnungen. zeigen Sie, dass die Menge $\mathbb{L}(F(x,y,z))$ "*im Wesentlichen endlich* ist, d.h. dass es im Raum $\mathbb{R}^3$ endlich viele Geraden $g_1, g_1, \ldots, g_r$ durch den Nullpunkt $(0,0,0) \in \mathbb{R}^3$ gibt so, dass

$$\mathbb{L}(F(x,y,z)) \subset \bigcup_{i=1} g_i.$$

D) Präzisieren Sie die Aussage aus Aufgabe C) wie folgt: Es gibt eine nichtnegative ganze Zahl $r \in \mathbb{N}_0$ und r paarweise verschiedene Tripel

$$(x_0^{[i]}, y_0^{[i]}, z_0^{[i]}) \in \mathbb{Z}^3 \setminus \{(0,0,0)\} \quad (i = 1, 2, \ldots r)$$

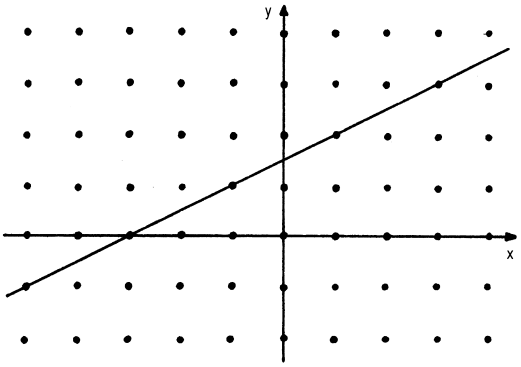
so, dass

(a) $x_0^{[i]}, y_0^{[i]}, z_0^{[i]}$ untereinander teilerfremd sind für alle $i \in \{1, 2, \ldots, r\}$;

(b) $\mathbb{L}(F(x,y,z)) = \bigcup_{i=1}^{r} \{(tx_0^{[i]}, ty_0^{[i]}, tz_0^{[i]}) \mid t \in \mathbb{Z} \setminus \{0\}\}$.

Lösungen einiger Aufgaben

Aufgaben 1.4 A) Siehe Zeichnung. Wegen $\mathrm{ggT}(-1,2) = 1$ und $1|3$ existieren nach 1.2 Lösungen. Wir wenden das Verfahren aus 1.3 an, um die Lösungsmenge $\mathbb{L}$ zu bestimmen. Wir suchen $u, v \in \mathbb{Z}$ mit $-u + 2v = 1$. Ausprobieren liefert $u = 1$ und $v = 1$, und es folgt $\mathbb{L} = \{(3 + 2t, 3 + t) | t \in \mathbb{Z}\}$.



Aufgabe 1.4 A)

B) Eine lineare diophantische Gleichung mit mindestens zwei Lösungen in

$$\{(x, y) | 0 \leq x \leq 2, 0 \leq y \leq 1\}$$

entspricht geometrisch einer Geraden, welche durch mindestens zwei der Gitterpunkte

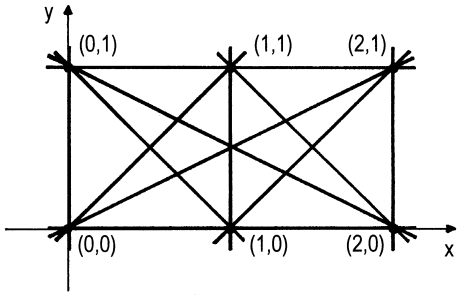
$$(0,0), (0,1), (1,0), (1,1), (2,0), (2,1)$$

geht. Wie man der Skizze entnimmt, gibt es elf solcher Geraden. Da die zugehörigen Gleichungen jeweils mit einer von 0 verschiedenen ganzen Zahl multipliziert werden können ohne dass sich dabei die Lösungsmenge ändert, erhalten wir die folgenden Typen

von Gleichungen, wobei $\lambda \in \mathbb{Z} \setminus \{0\}$.

I :	$\lambda x = 0$	V :	$\lambda y = \lambda$	IX :	$\lambda x - \lambda y = 0$
II :	$\lambda x = \lambda$	VI :	$\lambda x + 2\lambda y = 2\lambda$	X :	$\lambda x + \lambda y = 2\lambda$
III :	$\lambda x = 2\lambda$	VII :	$\lambda x - 2\lambda y = 0$	XI :	$\lambda x - \lambda y = \lambda$
IV :	$\lambda y = 0$	VIII :	$\lambda x + \lambda y = 0$		

Einen zwölften Typ Gleichung, der die Bedingungen erfüllt, liefert die Wahl $a = b = c = 0$.



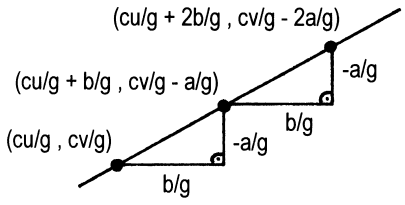
Aufgabe 1.4 B)

C) Damit überhaupt Lösungen existieren, muss $\mathrm{ggT}(a, b) = 1$ gelten. Ist (x, y) eine Lösung, so ist auch $(x + tb, y - ta)$ mit $t \in \mathbb{Z}$ eine Lösung. Aus der Skizze ist ersichtlich, das zwei verschiedene solche Lösungen minimalen Abstand haben, wenn $t = 1$ gilt. Ihr Abstand beträgt dann

$$\sqrt{(x - (x + b))^2 + (y - (y + a))^2} = \sqrt{a^2 + b^2}.$$

Es soll somit $\sqrt{a^2 + b^2} < 4$, also $a^2 + b^2 < 16$ gelten. Ausprobieren liefert für (a, b) die Möglichkeiten

$$(\pm 1, \pm 1),\ (\pm 1, \pm 2),\ (\pm 1, \pm 3),\ (\pm 2, \pm 1),\ (\pm 2, \pm 3),\ (\pm 3, \pm 1),\ (\pm 3, \pm 2).$$



Aufgabe 1.4 C)

D) Seien $g := \mathrm{ggT}(a, b)$ und $u, v \in \mathbb{Z}$ mit $au + bv = g$. Zwei „benachbarte“ Lösungen

haben die Form $(\frac{cu}{g}+\frac{tb}{g}, \frac{cv}{g}-\frac{ta}{g})$ und $(\frac{cu}{g}+\frac{(t+1)b}{g}, \frac{cv}{g}-\frac{(t+1)a}{g})$ mit $t \in \mathbb{Z}$ (s. Skizze zu C)). Ihr Abstand beträgt

$$\sqrt{\left(\frac{cu}{g}+\frac{tb}{g}-\left(\frac{cu}{g}+\frac{(t+1)b}{g}\right)\right)^2+\left(\frac{cv}{g}-\frac{ta}{g}-\left(\frac{cv}{g}-\frac{(t+1)a}{g}\right)\right)^2}=$$

$$\sqrt{\frac{a^2+b^2}{g^2}}=\frac{1}{g}\sqrt{a^2+b^2}.$$

E) a) Sei G die durch $ax+by=c$ definierte Gerade. Für einen beliebigen Punkt (x,y) auf G gilt $y=\frac{c}{b}-\frac{a}{b}x$, und somit beträgt sein Abstand vom Nullpunkt

$$f(x):=\sqrt{x^2+y^2}=\sqrt{\frac{a^2+b^2}{b^2}x^2-\frac{2ac}{b^2}x+\frac{c^2}{b^2}}.$$

Wir wollen einen Punkt $(x_0,y_0)\in G$ so bestimmen, dass sein Abstand von $(0,0)$ minimal wird. Dazu genügt es, wenn das Quadrat seinen Abstandes minimal wird, weswegen wir im obigen Ausdruck die Wurzel weglassen können. Bekanntlich ist x_0 die Nullstelle der Ableitung von f. Es gilt also $x_0=\frac{ac}{a^2+b^2}$, und es folgt $y_0=\frac{bc}{a^2+b^2}$. Einsetzen und umformen ergibt

$$f(x_0)=\sqrt{x^2+y^2}=\sqrt{\frac{c^2\left(a^2+b^2\right)}{\left(a^2+b^2\right)^2}}=\left|\frac{c\sqrt{a^2+b^2}}{a^2+b^2}\right|=|\delta|.$$

b) Sei weiterhin (x_0,y_0) ein Punkt auf G mit minimalem Abstand $|\delta|$ vom Nullpunkt. sei $g:=\mathrm{ggT}(a,b)$. Es bezeichne $d:=\frac{1}{g}\sqrt{a^2+b^2}$ den Abstand zwischen zwei „benachbarten“ Lösungen (vgl. D)). Läge keine Lösung in einem Abstand von höchstens $\frac{d}{2}$ von (x_0,y_0), so gäbe es zwei „benachbarte“ Lösungen mit einem Abstand grösser als d. Lägen drei Lösungen in einem Abstand von höchstens $\frac{d}{2}$ von (x_0,y_0), so wären zwei davon „benachbart“, hätten aber einen echt kleineren Abstand voneinander als d. Somit liegen mindestens eine und höchstens zwei Lösungen in einem Abstand von $\frac{d}{2}$ von (x_0,y_0). Da Abstände zwischen einer Geraden und einem Punkt jeweils rechtwinklig zur Geraden gemessen werden, liefert der Satz des Pythagoras die Behauptung.

F) Durch Ausprobieren findet man die Faktorisierung

$$2x^2-3y^2-5xy+x+11y-6=(2x+y-3)(x-3y+2).$$

Eine Lösung der gegebenen Gleichung ist ein Paar $(x,y)\in\mathbb{Z}^2$, welches eingesetzt in obigen Ausdruck 0 ergibt. Dies ist genau dann der Fall, wenn $2x+y-3=0$ oder $x-3y+2=0$. Somit sind diese beiden linearen diophantischen Gleichungen zu lösen. Für die erste Gleichung finden wir mit dem Verfahren aus 8.3 die Lösungsmenge

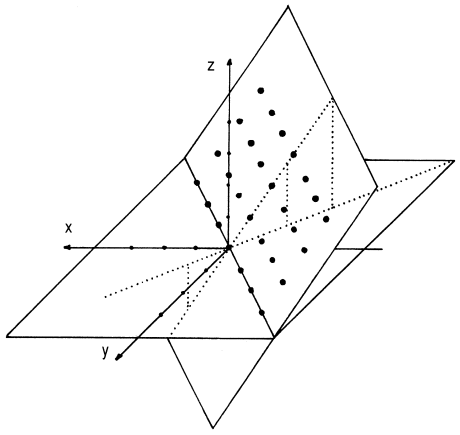
$$\mathbb{L}_1=\{(3+t,-3-2t)|t\in\mathbb{Z}\}.$$

Analog finden wir für die zweite Gleichung

$$\mathbb{L}_2 = \{(-8 - 3s, -2 - s) | s \in \mathbb{Z}\},$$

und es gilt für die Lösungsmenge $\mathbb{L}$ der gegebenen Gleichung $\mathbb{L} = \mathbb{L}_1 \cup \mathbb{L}_2$.

Aufgaben 1.6 A) Wir verwenden das Verfahren aus 1.5. Es gilt $g := \text{ggT}(1, 1) = 1$. Sei $f(z) := z$. Für jedes $z \in \mathbb{Z}$ gilt $g|f(z)$, weswegen für jede Wahl von z eine Lösung existiert. Mit $u = 1$ und $v = 0$ gilt $u+v = 1$ und wir erhalten $\mathbb{L} = \{(z+t, -t, z) | t, z \in \mathbb{Z}\}$.



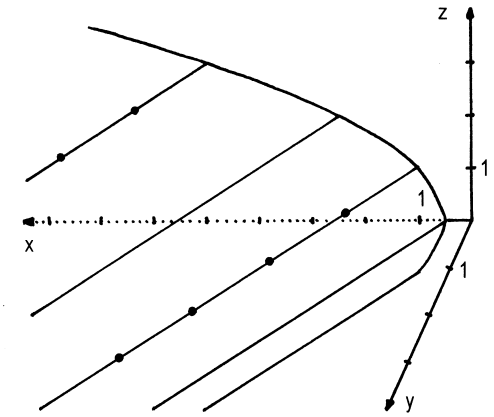
Aufgabe 1.6 A)

B) Wir verwenden das Verfahren aus 1.5. Es gilt $g := \text{ggT}(-1, 1) = 1$. Sei $f(z) := z^2$. Für jedes $z \in \mathbb{Z}$ gilt $g|f(z)$, weswegen für jede Wahl von z eine Lösung existiert. Mit $u = 0$ und $v = 1$ gilt $-u + v = 1$ und wir erhalten $\mathbb{L} = \{(t, z^2 + t, z) | t, z \in \mathbb{Z}\}$. Geometrisch liegt genau die Situation aus Abbildung 1.2 vor.
C) Wir verwenden das Verfahren von 1.5 und bestimmen zuerst $(u, v) \in \mathbb{Z}^2$ mit $2u - 6v = \text{ggT}(2, -6) = 2$. Das Paar $(u, v) = (4, 1)$ erfüllt dies, und wir erhalten damit die Lösungsmenge

$$\left\{ \left(\frac{z^2+1}{2} \cdot 4 + t \cdot \frac{-6}{2}, \frac{z^2+1}{2} \cdot 1 - t \cdot \frac{2}{2}, z \right) \middle| t, z \in \mathbb{Z} \wedge 2|z^2 + 1 \right\} =$$

$$\left\{ \left(2z^2 + 2 - 3t, \frac{z^2+1}{2} - t, z \right) \middle| t, z \in \mathbb{Z} \wedge z \text{ ungerade} \right\}.$$

D) Damit die Lösungsmenge leer ist, darf $g := \text{ggT}(5, -b) = \text{ggT}(5, b)$ für kein $z \in \mathbb{Z}$ ein Teiler von $f(z) := 10z^4 - 11$ sein. Es gilt sicher $g \in \{1, 5\}$. Für $g = 1$ gilt $g|f(z)$ für jedes $z \in \mathbb{Z}$. Also bleibt nur noch $g = 5$ übrig. Wegen $5|10z^4$ ist 5 für kein $z \in \mathbb{Z}$ ein



Aufgabe 1.6 C)

Teiler von $f(z)$. Die Bedingung $g = 5$ erreichen wir mit $b \in \{0, 5\}$.
Für die übrigen Fälle, das heisst für $b \in \{1, 2, 3, 4\}$, kann das Verfahren aus 1.5 angewendet werden und es ergeben sich die Lösungsmengen

$$\mathbb{L}_{b=1} = \{(10z^4 - t - 11, 40z^4 - 5t - 44, z)|t, z \in \mathbb{Z}\};$$

$$\mathbb{L}_{b=2} = \{(10z^4 - 2t - 11, 20z^4 - 5t - 22, z)|t, z \in \mathbb{Z}\};$$

$$\mathbb{L}_{b=3} = \{(-10z^4 + 3t + 11, -20z^4 - 5t + 22, z)|t, z \in \mathbb{Z}\};$$

$$\mathbb{L}_{b=4} = \{(10z^4 + 4t - 11, 10z^4 - 5t - 11, z)|t, z \in \mathbb{Z}\}.$$

Aufgaben 1.9 A) Für jedes $n \in \mathbb{N}$ mit $n \geq 3$ sind die Schnittpunkte mit den Koordinatenachsen die einzigen rationalen Punkte auf der n-ten Fermatkurve.
B) Wir nehmen an, es wäre $b := \sqrt[n]{1 - a^n} \in \mathbb{Q}$. Dann gälte $b \neq 0$. Es folgte $a^n + b^n = a^n + \left(\sqrt[n]{1 - a^n}\right)^n = a^n + 1 - a^n = 1$, also $(a, b) \in \mathbb{Q} \cap \mathbb{M}_n$ mit $ab \neq 0$ im Widerspruch zu A).
C) Für $a = \frac{3}{5}$ erhält man $\sqrt[2]{1 - a^2} = \sqrt[2]{1 - \frac{3^2}{5^2}} = \sqrt[2]{\frac{16}{25}} = \frac{4}{5} \in \mathbb{Q}$.
D) Ist $(a_n, a_n) \in \mathbb{M}_n$, so gilt $1 = a_n^n + a_n^n = 2a_n^n$, also $a_n = \sqrt[n]{\frac{1}{2}}$. Wird n beliebig gross, strebt $\frac{1}{n}$ gegen 0. Somit strebt $a_n = \left(\frac{1}{2}\right)^{\frac{1}{n}}$ gegen $\left(\frac{1}{2}\right)^0 = 1$, es gilt also $\lim_{n\to\infty}(a_n) = 1$.
E) Ist $(u, v_n) \in \mathbb{M}_n$, so gilt $v_n^n = 1 - u^n$, und es folgt $v_n = \sqrt[n]{1 - u^n}$. Wird n beliebig gross, so strebt u^n wegen $|u| < 1$ gegen 0. Somit strebt $1 - u^n$ gegen 1 und zudem $\frac{1}{n}$ gegen 0, also $\lim_{n\to\infty}(v_n) = 1$.
F) Ist $(u, w_k) \in \mathbb{M}_{2k+1}$, so gilt $w_k^{2k+1} = 1 - u^{2k+1}$. Wird k beliebig gross, so können wir wegen $|u| > 1$ den Summanden 1 vernachlässigen und erhalten $\lim_{k\to\infty}\left(\left(-u^{2k+1}\right)^{\frac{1}{2k+1}}\right) = \lim_{k\to\infty}(-u) = -u$.

Aufgaben 1.11 A) Die Werte von d sind klein, weswegen wir das Verfahren von 1.10 D) anwenden. Wir berechnen also die Werte von dy^2+1 für kleine $y \in \mathbb{N}$ und prüfen, ob $\sqrt{dy^2+1} \in \mathbb{N}$. Ist dies der Fall, so ist $(\sqrt{dy^2+1}, y)$ die kleinste nichttriviale Lösung der gegebenen Gleichung.
i) Es gelten $2 \cdot 1^2 + 1 = 3$, $2 \cdot 2^2 + 1 = 9$ und $\sqrt{9} = 3 \in \mathbb{N}$. Minimale Lösung: $(3, 2)$.
ii) Es gelten $3 \cdot 1^2 + 1 = 4$ und $\sqrt{4} = 2 \in \mathbb{N}$. Minimale Lösung: $(2, 1)$.
iii) Es gelten $7 \cdot 1^2 + 1 = 8$, $7 \cdot 2^2 + 1 = 29$, $7 \cdot 3^2 + 1 = 64$ und $\sqrt{64} = 8 \in \mathbb{N}$. Minimale Lösung: $(8, 3)$.
iv) Es gelten $6 \cdot 1^2 + 1 = 7$, $6 \cdot 2^2 + 1 = 25$ und $\sqrt{25} = 5 \in \mathbb{N}$. Minimale Lösung: $(5, 2)$.
v) Es gelten $8 \cdot 1^2 + 1 = 9$ und $\sqrt{9} = 3 \in \mathbb{N}$. Minimale Lösung: $(3, 1)$.
vi) Es gelten $10 \cdot 1^2 + 1 = 11$, $10 \cdot 2^2 + 1 = 41$, $10 \cdot 3^2 + 1 = 91$, $10 \cdot 4^2 + 1 = 161$, $10 \cdot 5^2 + 1 = 251$, $10 \cdot 6^2 + 1 = 361$ und $\sqrt{361} = 19 \in \mathbb{N}$. Minimale Lösung: $(19, 6)$.
D) $(d+1)^2 - d\left(\sqrt{d+2}\right)^2 = d^2 + 1 + 2d - d(d+2) = d^2 + 1 + 2d - d^2 - 2d = 1$.
I) i) Wegen $\sqrt{14+2} = 4 \in \mathbb{N}$ ist $(x_1, y_1) := (15, 4)$ nach Aufgabe D) eine Lösung von $x^2 - 14y^2 = 1$. Weitere Lösungen erhalten wir mit dem Verfahren von Aufgabe C) wie folgt:

$$x_2 := x_1^2 + 14y_1^2 = 449,\ y_2 := 2x_1y_1 = 120;$$

$$x_3 := x_1x_2 + 14y_1y_2 = 13455,\ y_3 := x_1y_2 + x_2y_1 = 3596.$$

Dies gibt die Lösungen $(449, 120)$ und $(13455, 3596)$.
ii) Wegen $\sqrt{34+2} = 6 \in \mathbb{N}$ ist $(x_1, y_1) := (35, 6)$ nach Aufgabe D) eine Lösung von $x^2 - 34y^2 = 1$. Weitere Lösungen erhalten wir mit dem Verfahren von Aufgabe C) wie folgt:

$$x_2 := x_1^2 + 34y_1^2 = 2449,\ y_2 := 2x_1y_1 = 420;$$

$$x_3 := x_1x_2 + 34y_1y_2 = 171395,\ y_3 := x_1y_2 + x_2y_1 = 29394.$$

Dies gibt die Lösungen $(2449, 420)$ und $(171395, 29394)$.

Aufgaben 2.2 A) Eine geschlossene Schnur mit 12, 30 oder 40 Knoten in regelmässigen Abständen erlaubt die Messung eines rechten Winkels . Beträgt die Anzahl der Knoten 60, so erhält man zwei wesentlich verschiedene Winkelmasse. Bei der Berechnung des Preises des Modelles Duplex werden offenbar beide möglichen Masse berechnet, was einer Gesamtzahl von 120 Knoten entspricht und bei einer Reduktion um 25% einen Preis von 90 ¶ ergibt.
B) Sei $(x, y, z) \in \mathbb{N}^3$ ein pythagoräisches Tripel mit $x \in \mathbb{P}$. Dann gilt $x^2 = z^2 - y^2 = (z+y)(z-y)$, und es folgt $z+y, z-y \in \mathbb{T}(x^2) = \{1, x, x^2\}$, da x eine Primzahl ist. Gälte $z+y = 1$, so folgte $z \notin \mathbb{N}$ oder $y \notin \mathbb{N}$. Gälte $z+y = x$ und somit $z-y = x$, so folgte $z+y = z-y$, also $y = 0 \notin \mathbb{N}$. Somit müssen $z+y = x^2$ und $z-y = 1$ gelten, woraus man sofort die Behauptung erhält.
C) Sei $(x, y, z) \in \mathbb{N}^3$ ein pythagoräisches Tripel mit $x \leq y$. Wir nehmen an, es gälte $x = y$. Dann folgte $z^2 = x^2 + y^2 = 2x^2$. Daraus erhielten wir durch Wurzelbildung

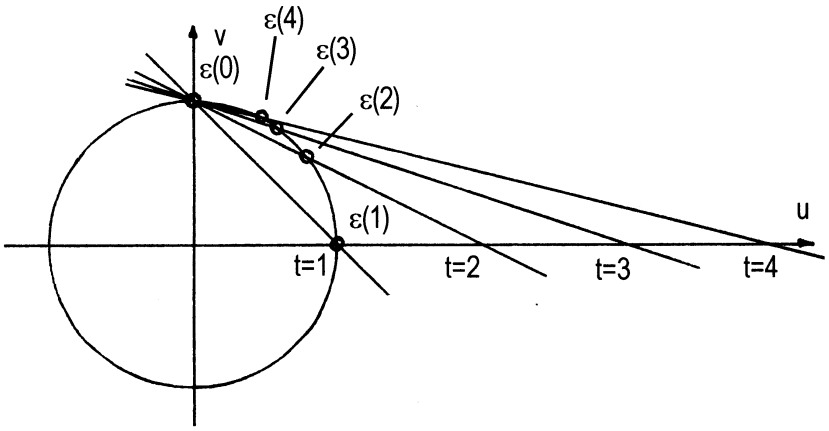
$\sqrt{2}x = \sqrt{2x^2} = \sqrt{z^2} = z \in \mathbb{N}$, also den Widerspruch $\sqrt{2} = \frac{z}{x} \in \mathbb{Q}$. Also gilt $x < y$. Wir nehmen an, es gälte $y \in \mathbb{P}$. Wenden wir 2.2 B) mit vertauschten Rollen von x und y an, so folgte $x = \frac{y^2-1}{2} < y$, also $y^2 - 2y + 1 = (y-1)^2 < 2$. Dies lieferte aber den Widerspruch $y = 1$.

Aufgaben 2.4 D) Die explizite Formel für die Abbildung ε aus 2.3 B)a) liefert

$$\varepsilon(0) = (0,-1),\ \varepsilon(1) = (1,0),\ \varepsilon(2) = \left(\frac{4}{5}, \frac{3}{5}\right),\ \varepsilon(3) = \left(\frac{3}{5}, \frac{4}{5}\right),$$

$$\varepsilon(4) = \left(\frac{8}{17}, \frac{15}{17}\right),\ \varepsilon(5) = \left(\frac{5}{13}, \frac{12}{13}\right).$$

Sicher gilt



Aufgabe 2.4 D)

$$\lim_{n\to\infty}(\varepsilon(n)) = \lim_{n\to\infty}\left(\frac{2n}{n^2+1}, \frac{n^2-1}{n^2+1}\right) = \left(\lim_{n\to\infty}\left(\frac{2n}{n^2+1}\right), \lim_{n\to\infty}\left(\frac{n^2-1}{n^2+1}\right)\right).$$

Die Summanden $+1$ und -1 können für genügend grosse n vernachlässigt werden. Durch Kürzen erhalten wir somit

$$\lim_{n\to\infty}(\varepsilon(n)) = \left(\lim_{n\to\infty}\left(\frac{2}{n}\right), \lim_{n\to\infty}(1)\right) = (0,1) = S,$$

was sich auch aufgrund der Skizze vermuten lässt (vgl. die geometrische Konstruktion der Abbildung ε in 2.3 A)).

E) Sei $n \in \mathbb{Z}$. Wegen

$$(2n)^2 + \left(n^2-1\right)^2 = 4n^2 + n^4 + 1 - 2n^2 = n^4 + 2n^2 + 1 = \left(n^2+1\right)^2$$

gilt für $(x, y, z) := (2n, n^2 - 1, n^2 + 1)$ die Gleichung $x^2 + y^2 = z^2$. Gilt zusätzlich $n \geq 2$, so folgt $(x, y, z) \in \mathbb{N}^3$, und (x, y, z) ist ein pythagoräisches Tripel.

Aufgaben 2.7 D) Wir betrachten hier nur das Produkt der ersten vier Primzahlen. Ein analoges Vorgehen löst aber auch die Aufgabe für acht Primfaktoren.
Sei also $u = 2 \cdot 3 \cdot 5 \cdot 7 = 210$. Nach 2.7 A) müssen wir teilerfremde $m, k \in \mathbb{Z}$ mit $m < k < 2m$ bestimmen so, dass k ungerade ist und dass $u = 2mk$. Dies bedeutet aber, dass $2mk = 210$, also dass $mk = 105$. Es folgt aus der obigen Ungleichungskette durch Multiplikation mit m, dass $m^2 < 105 < 2m^2$. Wurzelziehen erlaubt nun die Abschätzungen $m \leq 10 < \sqrt{2}m$. Weiter muss $m \in \{3, 3 \cdot 5, 3 \cdot 5 \cdot 7, 5, 5 \cdot 7, 7\}$ gelten. Wegen $m \leq 10$ erhalten wir damit $m \in \{3, 5, 7\}$. Aber in diesen drei Fällen gilt $\sqrt{2}m < 10$. Also gibt es kein primitives und somit überhaupt kein pythagoräisches Tripel mit Umfang 210.
E) i) Sei $n \in \mathbb{N}_{\geq 2}$. Dann gilt nach Definition des Umfanges eines pythagoräischen Tripels $x_n + y_n + z_n = 2^n \left(2^{n-1} + 1\right)$. Weil (x_n, y_n, z_n) primitiv ist, gibt es nach dem Satz von Diophantos zwei teilerfremde Zahlen $m, k \in \mathbb{N}$ mit $k < m$, wovon eine gerade und die andere ungerade ist so, dass

$$(x_n, y_n, z_n) = \left(2mk, m^2 - k^2, m^2 + k^2\right).$$

Es folgt

$$2^n \left(2^{n-1} + 1\right) = 2mk + m^2 - k^2 + m^2 + k^2 = 2m(m + k),$$

das heisst

$$2^{n-1} \left(2^n + 1\right) = m(m + k).$$

Weil $m + k$ ungerade ist, folgt $2^{n-1} | m$, also $m = 2^{n-1} l$ für ein $l \in \mathbb{N}$. Wir erhalten

$$2^{n-1} + 1 = l(m + k) = l \left(2^{n-1} l + k\right),$$

was wegen $l, k \in \mathbb{N}$ nur geht, wenn $l = k = 1$. Schliesslich erhalten wir

$$(x_n, y_n, z_n) = \left(2^n, 2^{2n-2} - 1, 2^{2n-2} + 1\right).$$

ii) Es gilt $\frac{y_n}{x_n} = \frac{2^{2n-2}-1}{2^n}$. Für genügend grosse n kann der Summand -1 vernachlässigt werden, und Kürzen liefert

$$\lim_{n \to \infty} \left(\frac{y_n}{x_n}\right) = \lim_{n \to \infty} \left(2^{n-2}\right) = \infty.$$

Analog erhält man

$$\lim_{n \to \infty} \left(\frac{z_n}{x_n}\right) = \infty.$$

Es gilt $\frac{z_n}{y_n} = \frac{2^{2n-2}+1}{2^{2n-2}-1}$. Für genügend grosse n können die Summanden $+1$ und -1 vernachlässigt werden, und Kürzen liefert

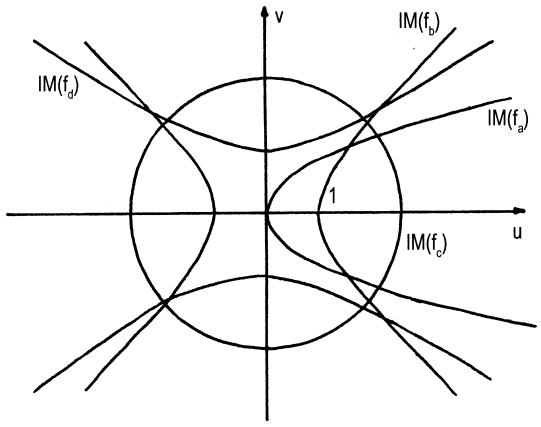
$$\lim_{n\to\infty}\left(\frac{z_n}{y_n}\right) = \lim_{n\to\infty}(1) = 1.$$

Aufgaben 2.9 A) Mit Hilfe des Satzes von Diophantos bestimmt man alle primitiven pythagoräischen Tripel, deren Umfang höchstens 60 beträgt. Es sind dies $(4,3,5)$, $(8,15,17)$, $(12,5,13)$ und $(24,7,25)$. Ist (x,y,z) ein pythagoräisches Tripel, so ist $\left(\frac{x}{z},\frac{y}{z}\right)$ ein rationaler Punkt auf dem Einheitskreis, und es gilt $(x,y,z) = \left(z\frac{x}{z}, z\frac{y}{z}, z\right)$. Die Abbildung ι aus 2.3 B)b), welche die Umkehrabbildung von ε ist, liefert zu jedem solchen rationalen Punkt $\left(\frac{x}{z},\frac{y}{z}\right)$ ein $t = \iota\left(\frac{x}{z},\frac{y}{z}\right) \in \mathbb{Q}$ mit $\left(\frac{x}{z},\frac{y}{z}\right) = (u(t),v(t))$, also mit $(x,y,z) = (zu(t), zv(t), z)$ wie gewünscht. Wie man leicht sieht, wird hierbei zwei Tripeln der Form (x,y,z) und (kx,ky,kz) mit $k \in \mathbb{N}$ dasselbe t zugeordnet. Somit können wir uns auf die schon bestimmten primitiven pythagoräischen Tripel beschränken.
Für $(x,y,z) = (4,3,5)$ finden wir $\left(\frac{x}{z},\frac{y}{z}\right) = \left(\frac{4}{5},\frac{3}{5}\right)$ und damit $\iota\left(\frac{4}{5},\frac{3}{5}\right) = \frac{\frac{4}{5}}{1-\frac{3}{5}} = 2$. Analog erhält man für die übrigen primitiven pythagoräischen Tripel in der obenstehenden Reihenfolge für t die Werte 4, $\frac{3}{2}$ und $\frac{4}{3}$.

Aufgaben 2.12 C) Setzt man $z = 1$, so errät man leicht eine Lösung indem man x oder y gleich 0 oder 1 wählt. Dies ergibt zum Beispiel: a) $(1,0,1)$; b) $(1,0,1)$; c) $(0,0,1)$; d) $(2,1,1)$; f) $(1,1,1)$.
D) Die Gleichung e) liefert für $z = 1$ eine Pell'sche Gleichung. Das Paar $(1,0)$ ist eine Lösung jeder Pell'schen Gleichung, und so finden wir die Lösung $(1,0,1)$.

Aufgaben 2.14 B) Es gelten $f_a(u,v) = u - v^2$, $f_b(u,v) = u^2 - v^2 - 1$, $f_c(u,v) = u^2 + v^2 - 7$ und $f_d(u,v) = -u^2 + 2v^2 - 3$. $\mathbb{M}(f_a)$ ist eine Parabel parallel zur u-Achse mit Scheitelpunkt im Ursprung. $\mathbb{M}(f_b)$ ist eine gleichseitige Hyperbel mit Mittelpunkt im Ursprung und Halbachsen (!) der Länge 1. $\mathbb{M}(f_c)$ ist ein Kreis um den Ursprung mit Radius $\sqrt{7}$. $\mathbb{M}(f_d)$ ist eine Hyperbel mit Mittelpunkt im Ursprung und Halbachsen der Längen $\sqrt{3}$ und $\sqrt{\frac{3}{2}}$.

Aufgaben 2.17 A) a) Wir behaupten, es sei $\mathbb{L} := \mathbb{L}\left(x^2 + y^2 - 3z^2\right) = \emptyset$ und gehen vor wie in 2.15. Wir nehmen an, es gäbe ein $(x,y,z) \in \mathbb{L}$. Ohne Einschränkung könnten wir annehmen, x, y und z hätten keinen gemeinsamen Primfaktor. Wir fänden also $m,n,r,s \in \mathbb{Z}$ mit $0 \le r,s \le 2$ und $(r,s) \neq (0,0)$ so, dass $x = 3m + r$ und $y = 3n + s$ gälten. Wegen $(x,y,z) \in \mathbb{L}$ erhielten wir $3z^2 = x^2 + y^2 = (3m+r)^2 + (3n+s)^2 = 3\left(3m^2 + 2mr + 3n^2 + 2ns\right) + r^2 + s^2$, also $3 | r^2 + s^2$. Man sieht aber leicht (zum Beispiel anhand einer Tabelle wie in 2.15), dass dies für keine Wahl von (r,s) mit $0 \le r,s \le 2$ mit $(r,s) \neq (0,0)$ erfüllt wäre, und somit erhielten wir einen Widerspruch. Also folgt die Behauptung.



Aufgabe 2.14 B)

b) $\mathbb{M}\,(u^2+v^2-3)$ ist ein Kreis mit Mittelpunkt im Ursprung und Radius $\sqrt{3}$.
B) Wir formulieren das Vorgehen von 2.15 allgemein. Für

$$(x,y,z) \in \mathbb{L}_c := \mathbb{L}\left(x^2+y^2-cz^2\right)$$

so, dass x, y und z keinen gemeinsamen Primfaktor haben, gibt es $m,n,r,s \in \mathbb{Z}$ mit $0 \le r,s \le c-1$, $(r,s) \neq (0,0)$ so, dass $x = cm+r$ und $y = cn+s$, und weiter gilt

$$(*) \qquad cz^2 = x^2+y^2 = c\left(cm^2+2mr+cn^2+2ns\right)+r^2+s^2,$$

also $c|r^2+s^2$. Wir stellen eine Tabelle mit den Werten von r^2+s^2 auf, welche wir aus Symmetriegründen nicht vollständig auszufüllen brauchen.

	0	1	2	3	4	5	6	7	8	9
0	0									
1	1	2								
2	4	5	8							
3	9	10	13	18						
4	16	17	20	25	32					
5	25	26	29	34	41	50				
6	36	37	40	45	52	61	72			
7	49	50	53	58	65	74	85	98		
8	64	65	68	73	80	89	100	113	128	
9	81	82	85	90	97	106	107	145	145	162

Betrachtet man nun einen quadratischen Ausschnitt dieser Tabelle, ausgehend von der linken oberen Ecke mit einer Seitelänge von c Zellen, so genügt es zu sehen, dass c keinen der darin enthaltenen von 0 verschiedenen Einträge teilt. Dies ist für alle $c \in \{1,3,7\}$ der Fall, und es folgt also $\mathbb{L}_1 = \mathbb{L}_3 = \mathbb{L}_7 = \emptyset$.
In den Fällen $c \in \{2,4,5,8,9,10\}$ finden wir ein $(x,y,z) \in \mathbb{L}_c$, indem wir im entsprechenden Tabellenausschnitt einen Eintrag wählen, der ein Vielfaches von c ist. Wir bestimmen die entsprechenden Werte für r und s und setzen $x = r$ und $y = s$, was in

den Darstellungen $x = cm + r$ und $y = cn + s$ der Wahl von $m = n = 0$ entspricht. Nun findet man leicht ein passendes z so, dass $(x, y, z) \in \mathbb{L}_c$. Konkret erhält man zum Beispiel $(1, 1, 1) \in \mathbb{L}_2$, $(2, 0, 1) \in \mathbb{L}_4$, $(2, 1, 1) \in \mathbb{L}_5$, $(2, 2, 1) \in \mathbb{L}_8$, $(3, 0, 1) \in \mathbb{L}_9$ und $(3, 1, 1) \in \mathbb{L}_{10}$.
Übrig bleibt jetzt nur noch der Fall $c = 6$. Die obenstehende Tabelle liefert nicht direkt einen Widerspruch, denn es gilt $6|(3^2 + 3^2)$. Die dadurch bestimmte Wahl von $(r, s) = (3, 3)$ ist aber die einzig mögliche. Nach $(*)$ folgt

$$6(6(m(m + 1) + n(n + 1))) + 18 = 6z^2,$$

nach Kürzen mit 6 also

$$6(m(m + 1) + n(n + 1)) + 3 = z^2.$$

Deswegen sind z^2 und somit auch z ein Vielfaches von 3. Es gibt also ein $w \in \mathbb{Z}$ mit $z = 3w$. Damit können wir obige Gleichung mit 3 kürzen und erhalten

$$2(m(m + 1) + n(n + 1)) = 3w^2 - 1.$$

Die linke Seite dieser Gleichung ist sicher gerade, und deshalb sind $3w^2$ und damit auch w ungerade. Dies heisst, dass es ein $t \in \mathbb{Z}$ gibt mit $w = 2t + 1$. Damit erhalten wir

$$2(m(m + 1) + n(n + 1)) = 3(2t + 1)^2 - 1 = 12t^2 + 12t + 2.$$

Dividieren wir diese Gleichung mit 2, so folgt

$$m(m + 1) + n(n + 1) = 6t^2 + 6t + 1 = 6t(t + 1) + 1.$$

Hierbei ist aber die linke Seite gerade und die rechte Seite ungerade. Dieser Widerspruch zeigt, dass $\mathbb{L}_6 = \emptyset$ gilt.