Inhaltsverzeichnis

Ein Ausflug in die p-adische Welt

Annette Werner

3. März 2011

1 Annette Werner: Ein Ausflug in die p-adische Welt

1.1 Abstände in der p-adischen Welt

Vermutlich hat jeder schon einmal mit einem Lineal oder einem Maßband Längen oder Abstände ausgemessen. Den Abstand, den diese Hilfmittel messen, kann man mathematisch als eine Funktion d auffassen, die zwei Punkten x und y des Raumes eine reelle Zahl $d(x, y)$ zuordnet, die folgenden Gesetzen genügt:

1) Es ist immer $d(x, y) \geq 0$, wobei $d(x, y) = 0$ nur gilt, wenn $x = y$ ist.

2) Es ist $d(x, y) = d(y, x)$ für alle Punkte x und y.

3) Sind x, y und z drei Punkte, dann gilt $d(x, z) \leq d(x, y) + d(y, z)$.

Dieser Abstandsbegriff wird in dem Beitrag von Gabriele Nebe über Kugelpackungen untersucht und verallgemeinert.

In der Mathematik interessiert man sich aber auch für andere Abstände, die durch ihre Anwendungen in der Zahlentheorie interessant sind. Dazu fixieren wir eine Primzahl p – dies ist das p, das in der Überschrift dieses Beitrags auftaucht. Dabei ist eine ganze Zahl p, die größer oder gleich 2 ist, eine Primzahl, falls sie nur die Teiler 1 und p hat. Beispielsweise sind

$$2, 3, 5, 7, 11, 13, 17, 23, 29, 31, 37, 41$$

Primzahlen, aber 57 ist keine Primzahl, da sie außer durch 1 und 57 zum Beispiel auch noch durch 3 teilbar ist.

Primzahlen faszinieren Mathematikerinnen und Mathematiker schon seit der Antike. Sie spielen eine wichtige Rolle in vielen tiefen Vermutungen der modernen Mathematik, etwa in der Riemann'schen Vermutung oder in der Vermutung von Birch und Swinnerton-Dyer, die in dem Beitrag von Annette Huber erklärt wird. Gleichzeitig tauchen sie in modernen Computerprogrammen auf, etwa in Verschlüsselungsverfahren, wie sie in dem Beitrag von Priska Jahnke beschrieben werden.

Man kann jede ganze Zahl als Produkt von Primzahlen (eventuell mit einem Vorzeichen) schreiben. Daher sind die Primzahlen die Bausteine, aus denen die Welt der ganzen Zahlen zusammengesetzt ist. So ist etwa $1400 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 7 = 2^3 \cdot 5^2 \cdot 7$.

Schon dem antiken Mathematiker Euklid war bekannt, dass es unendlich viele Primzahlen gibt. Um dies zu zeigen, nehmen wir an, es gebe nur endlich viele Primzahlen. Diese können wir dann durchnummerieren und $p_1, p_2, \ldots, p_n$ nennen. Dann betrachten wir die Zahl $N = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$. Da N größer als eins ist, gibt es eine Primzahl, die ein Teiler von N ist. Diese Primzahl ist eine der Zahlen $p_1, p_2, \ldots, p_n$, nennen wir sie p_i. Da p_i sowohl N als auch das Produkt $p_1 \cdot p_2 \cdot \cdots \cdot p_n$ teilt, ist p_i auch ein Teiler der

Differenz $1 = N - p_1 \cdot p_2 \cdot \cdots \cdot p_n$. Das kann aber nicht sein! Also gibt es unendlich viele Primzahlen.

Wir schreiben für eine beliebige ganze Zahl $m \neq 0$ die Primfaktorzerlegung als

$$m = \pm \prod_{p \text{ Primzahl}} p^{v_p(m)}.$$

Hier ist $v_p(m)$ die größte ganze Zahl, für die $p^{v_p(m)}$ ein Teiler von m ist. Das Produkt läuft hier formal über alle Primzahlen, aber natürlich ist jede Zahl m nur durch endlich viele Primzahlen p teilbar. Für alle bis auf endlich viele Primzahlen p gilt also $v_p(m) = 0$, denn $p^0 = 1$ ist ja auf jeden Fall ein Teiler von m. In unserem Beispiel $m = 1400$ ist etwa

$$v_2(1400) = 3, \quad v_3(1400) = 0, \quad v_5(1400) = 2, \quad v_7(1400) = 1.$$

Es ist leicht nachzuprüfen, dass immer $v_p(mn) = v_p(m) + v_p(n)$ gilt.

Wir fixieren jetzt eine Primzahl p, die für den ganzen Rest dieses Artikel unverändert bleibt. Mit ihrer Hilfe definieren wir einen neuen Abstand zwischen zwei ganzen Zahlen m und n, den wir den **p-adischen Abstand** nennen:

Definition 1.1 *i) Ist $m = n$, so setzen wir $d_p(m, n) = 0$.*
ii) Ist $m \neq n$, so definieren wir $d_p(m, n) = \frac{1}{p^{v_p(m-n)}}$.

Falls $m-n$ nicht durch p teilbar ist, so gilt also $v_p(m-n) = 0$ und somit $d_p(m, n) = 1$. Wir können beispielsweise ausrechnen

$$d_2(1, 9) = 1/8 \text{ und } d_3(23, 2) = 1/3.$$

Außerdem gilt $d_2(m, n) = 1$, wann immer m gerade und n ungerade ist (oder umgekehrt), denn in diesen Fällen ist die Differenz $m - n$ eine ungerade Zahl.

Wir sehen also, dass Zahlen, die bezüglich unseres gewöhnlichen Abstandsbegriffs sehr weit auseinanderliegen, bezüglich des p-adischen Abstandsbegriffs sehr nahe beieinander sein können und umgekehrt. Die folgende Abbildung zeigt den 3-adischen Abstand zur Null, also $d_3(m, 0) = 1/3^{v_3(m)}$, aller Zahlen von eins bis dreißig.

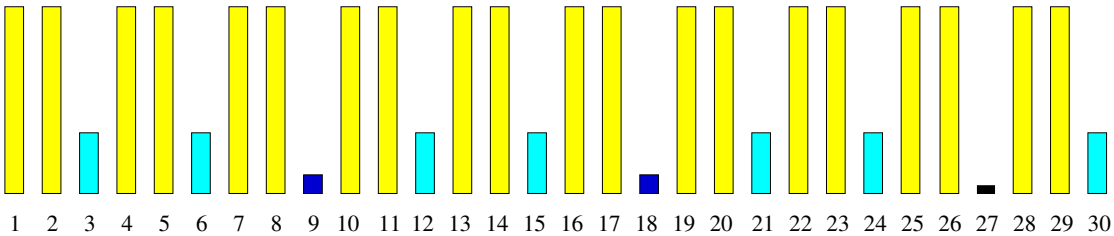

Abbildung 1.1: Größenverhältnisse in der 3-adischen Welt

Der p-adische Abstandsbegriff erfüllt ebenfalls die Bedingungen 1) bis 3), die wir zu Beginn erklärt haben. Er verdient es also in der Tat, als Abstand bezeichnet zu werden. Die ersten beiden Bedingungen sind sehr einfach nachzuprüfen. Wir schauen uns die dritte Bedingung, die sogenannte Dreiecksungleichung, näher an. Dazu betrachten wir drei ganze Zahlen k, m und n. Es sei v die kleinere der beiden Zahlen $v_p(k-m)$ und $v_p(m-n)$. Dann teilt p^v sowohl $k-m$ als auch $m-n$. Daher ist p^v auch ein Teiler der Summe $(k-m)+(m-n)=k-n$. Demnach gilt $v \leq v_p(k-n)$. Nun drehen sich beim Übergang von v zu $1/p^v$ alle Ungleichungen um, daher ist $1/p^v$ die größere der beiden Zahlen $d_p(k,m)=1/p^{v_p(k-m)}$ und $d_p(m,n)=1/p^{v_p(m-n)}$. Das schreiben wir als $1/p^v=\max\{d_p(k,m),d_p(m,n)\}$. Aus $v \leq v_p(k-n)$ folgt nun

$$d_p(k,n)=1/p^{v_p(k-n)} \leq 1/p^v=\max\{d_p(k,m),d_p(m,n)\}.$$

Wir erhalten also eine verschärfte Form der Dreiecksungleichung: Für drei ganze Zahlen k,m,n gilt

$$d_p(k,n) \leq \max\{d_p(k,m),d_p(m,n)\}.$$

Daraus folgt natürlich die gewohnte Dreiecksungleichung

$$d_p(k,n) \leq d_p(k,m)+d_p(m,n).$$

Unser Beweis der verschärften Dreiecksungleichung zeigt noch etwas mehr. Falls $d_p(k,m) \neq d_p(m,n)$ gilt, dann folgt sogar

$$d_p(k,n)=\max\{d_p(k,m),d_p(m,n)\}.$$

In diesem Fall kann nämlich keine größere p-Potenz als p^v die Summe $(k-m)+(m-n)=k-n$ teilen. (Überlegen Sie sich einmal, wieso das nicht möglich ist!)

Wir können nun den p-adischen Abstandsbegriff problemlos auf die rationalen Zahlen übertragen. Eine rationale Zahl ist ein Bruch m/n, wobei der Zähler m und der Nenner n ganze Zahlen sind und $n \neq 0$ gilt. Die Menge der rationalen Zahlen bezeichnet man mit $\mathbb{Q}$.

Wir definieren nun

$$v_p(m/n)=v_p(m)-v_p(n)$$

für jede rationale Zahl $m/n \neq 0$. Beispielsweise ist $v_2(1/2)=-1$. Jetzt definieren wir den Abstand von zwei rationalen Zahlen r und s wie oben als $d_p(r,s)=0$, falls $r=s$, und als

$$d_p(r,s)=1/p^{v_p(r-s)},$$

falls r ungleich s ist. Beispielsweise gilt $d_2(1/2,0)=2$.

Nun betrachten wir alle rationalen Zahlen, die von 0 höchstens den Abstand 1 haben:

$$R=\{r \in \mathbb{Q} : d_p(r) \leq 1\}=\{r \in \mathbb{Q} : v_p(r) \geq 0\}.$$

Streng genommen müssten wir hier R_p statt R schreiben, denn diese Teilmenge hängt ja von unserer Ausgangsprimzahl p ab. Wir verzichten aber darauf, damit unsere Formeln nicht zu unübersichtlich werden. Die Teilmenge R der rationalen Zahlen ist also ein p-adischer Verwandter der Menge aller rationalen Zahlen, die im Einheitsintervall liegen, also von $[-1,1] \cap \mathbb{Q} = \{r \in \mathbb{Q} : |r| \leq 1\}$. Multipliziert man zwei Zahlen dieses rationalen Einheitsintervalls, dann liegt das Ergebnis ebenfalls in $[-1,1]$. Addiert man allerdings zwei Zahlen des rationalen Einheitsintervalls, dann kann das Ergebnis auch außerhalb von $[-1,1]$ liegen.

Die starke Dreiecksungleichung in der p-adischen Welt sorgt dafür, dass die Teilmenge R der rationalen Zahlen sich besser verhält. Sind nämlich r und s zwei rationale Zahlen, die in R liegen, dann schreiben wir $r = k/l$ und $s = m/n$ mit ganzen Zahlen k, l, m und n, wobei die Nenner l und n natürlich nicht null sein dürfen. Wegen $d_p(r) \leq 1$ gilt $v_p(r) = v_p(k) - v_p(l) \geq 0$, also $v_p(k) \geq v_p(l)$. Analog ist $v_p(m) \geq v_p(n)$. Nun rechnen wir

$$r + s = \frac{k}{l} + \frac{m}{n} = \frac{kn + ml}{ln}.$$

Nach der verschärften Dreiecksungleichung ist $v_p(kn + ml)$ mindestens so groß wie der kleinere der Werte $v_p(kn)$ und $v_p(ml)$. Da $v_p(k) \geq v_p(l)$ und $v_p(m) \geq v_p(n)$ ist, können wir diese Werte folgendermaßen abschätzen:

$$v_p(kn) = v_p(k) + v_p(n) \geq v_p(l) + v_p(n) \text{ und } v_p(ml) = v_p(m) + v_p(l) \geq v_p(n) + v_p(l).$$

Also gilt auf jeden Fall $v_p(kn + ml) \geq v_p(n) + v_p(l) = v_p(nl)$, woraus in der Tat folgt, dass $r + s$ in R liegt.

Es ist außerdem leicht einzusehen, dass mit zwei Zahlen r und s auch das Produkt rs in R liegt. Die Teilmenge R von $\mathbb{Q}$ enthält also 0 und 1 und mit je zwei Elementen außerdem auch deren Summe und Produkt.

1.2 p-adische Gitter in der Ebene

Nun betrachten wir sogenannte Vektoren über $\mathbb{Q}$. Genauer gesagt, interessiert uns hier die rationale Ebene

$$\mathbb{Q}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : x, y \in \mathbb{Q} \right\}.$$

Dies ist derjenige Teil der gewöhnlichen Koordinatenebene, der aus allen Punkten besteht, die nur rationale Koordinaten haben. Wir nennen die Elemente in $\mathbb{Q}^2$ auch Vektoren. Man kann jeden solchen Vektor $\begin{pmatrix} x \\ y \end{pmatrix}$ mit einer rationalen Zahl a multiplizieren. Das liefert den Vektor $\begin{pmatrix} ax \\ ay \end{pmatrix}$. Zeichnen wir diesen Vektor in die Ebene ein, so entsteht

er aus dem ursprünglichen Vektor durch eine Streckung (wenn $a \geq 1$) oder eine Stauchung (wenn $0 \leq a < 1$) oder eine Streckung beziehungsweise Stauchung des um 180 Grad gedrehten Vektors (wenn $a < 0$).

Es seien v und w zwei Vektoren in $\mathbb{Q}^2$, die nicht auf einer gemeinsamen Geraden durch den Nullpunkt liegen. Dies bedeutet, dass weder v noch w der Nullpunkt ist und dass es keine Zahl $a \in \mathbb{Q}$ gibt mit $av = w$. Dann betrachten wir die Teilmenge

$$L = Rv + Rw = \{av + bw : a, b \in R\}.$$

Die Menge L besteht also aus allen sogenannten Linearkombinationen der Vektoren v und w, wobei aber nur Faktoren aus R, nicht aus ganz $\mathbb{Q}$, zugelassen sind. Wir sagen dann, dass L von den Vektoren v und w erzeugt ist. Jede Teilmenge von $\mathbb{Q}^2$ der Form $Rv + Rw$ für zwei Vektoren v und w, die nicht auf einer gemeinsamen Geraden durch den Nullpunkt liegen, nennen wir ein **Gitter** in $\mathbb{Q}^2$. Es gibt viele verschiedene Paare von Vektoren, die dasselbe Gitter erzeugen. So ist das Gitter $L = Rv + Rw$ zum Beispiel nicht nur von v und w, sondern etwa auch von v und $v + w$ erzeugt.

Jetzt betrachten wir quadratische Matrizen mit Einträgen in den rationalen Zahlen. Eine solche Matrix ist ein quadratisches Schema von vier Zahlen a, b, c, d in $\mathbb{Q}$:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Wir können jede solche Matrix A auf folgende Weise mit einem Vektor $v = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Q}^2$ multiplizieren:

$$A \cdot v = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Die Multiplikation mit der Matrix $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ bewirkt hierbei einfach die Multiplikation mit der Zahl a, also, wie wir oben gesehen haben, für positives a eine Streckung oder Stauchung des Vektors und für negatives a eine Streckung oder Stauchung des um 180 Grad gedrehten Vektors. Für $a = 1$ lässt die Multiplikation mit dieser Matrix alle Vektoren invariant. Die zugehörige Matrix

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

heißt die Einheitsmatrix. Die Multiplikation mit $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ bewirkt eine Drehung um 90 Grad im Uhrzeigersinn.

Zwei quadratische Matrizen kann man folgendermaßen multiplizieren:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Die Multiplikation mit der Einheitsmatrix E ändert dabei eine Matrix nicht, das heißt, es gilt für jede quadratische Matrix A, dass $A \cdot E = E \cdot A = A$ ist.

Durch manche Matrizen kann man sogar teilen. Hierfür ist die sogenannte Determinante der Matrix eine wichtige Kennzahl. Ist A wie oben eine quadratische Matrix mit den Einträgen a, b, c und d, so heißt die Zahl $ad - bc$ die Determinante von A. Ist die Determinante von A ungleich null, so können wir die Matrix

$$B = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

betrachten. Es ist eine gute Übungsaufgabe, nachzuprüfen, dass $A \cdot B = B \cdot A = E$ gilt. Aus diesem Grund heißt die Matrix B inverse Matrix zu A. Sie spielt die Rolle des Kehrwerts von A.

Mit Hilfe der inversen Matrix wollen wir nun verschiedene Koordinatensysteme der Ebene untersuchen. Dazu betrachten wir zwei Vektoren v' und w' in $\mathbb{Q}^2$, die nicht auf einer gemeinsamen Geraden durch den Nullpunkt liegen. Wir schreiben

$$v' = \begin{pmatrix} a \\ c \end{pmatrix} \quad \text{und} \quad w' = \begin{pmatrix} b \\ d \end{pmatrix}.$$

Da v' und w' nicht auf einer gemeinsamen Geraden durch den Nullpunkt liegen, ist $ad - bc \neq 0$. Daher besitzt die Matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

eine inverse Matrix B. Nun sei

$$v = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Q}^2$$

ein beliebiger Vektor der rationalen Koordinatenebene $\mathbb{Q}^2$. Wir berechnen den Vektor

$$B \cdot v = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \frac{dx-by}{ad-bc} \\ \frac{-cx+ay}{ad-bc} \end{pmatrix}.$$

Die Einträge dieses Vektors geben die Koordinaten von v bezüglich des neuen Koordinatensystems (v', w') an, das heißt, es gilt

$$v = \frac{dx-by}{ad-bc}\, v' + \frac{-cx+ay}{ad-bc}\, w',$$

wie man durch Nachrechnen leicht bestätigen kann.

Wir haben also gesehen, dass jedes Paar von Vektoren (v', w'), die nicht auf einer gemeinsamen Geraden durch den Nullpunkt liegen, als Koordinatensystem der rationalen

Ebene $\mathbb{Q}^2$ verwendet werden kann, das heißt, für jeden Vektor $v \in \mathbb{Q}^2$ gibt es zwei rationale Zahlen α und β (die sogenannten (v', w')-Koordinaten), für die $v = \alpha v' + \beta w'$ gilt.

Nun kommen wir noch einmal zurück zur Determinante. Durch Einsetzen der Formel für die Determinante kann man nachprüfen, dass für zwei beliebige quadratische Matrizen A und B die Determinante des Produktes $A \cdot B$ gleich dem Produkt der Determinante von A mit der Determinante von B ist. Diese Berechnung überlassen wir der Leserin oder dem Leser als Übungsaufgabe. Daraus folgt, dass das Produkt von zwei Matrizen, deren Determinanten beide ungleich null sind, ebenfalls eine Determinante ungleich null hat. Daher bildet die Menge $GL_2(\mathbb{Q})$ aller Matrizen mit Determinante ungleich null zusammen mit dem Matrixprodukt eine sogenannte Gruppe. Über Gruppen kann man mehr in Rebecca Waldeckers Beitrag in diesem Band erfahren.

Mit $SL_2(\mathbb{Q})$ bezeichnen wir die Menge aller quadratischen Matrizen, deren Determinante gleich eins ist. Dann ist $SL_2(\mathbb{Q})$ eine Teilmenge der Gruppe $GL_2(\mathbb{Q})$. Nun hat das Produkt zweier Matrizen mit Determinante eins nach der obigen Übungsaufgabe auch wieder Determinante eins. Auch die Menge $SL_2(\mathbb{Q})$ ist eine Gruppe unter der Matrixmultiplikation.

1.3 Die Geometrie des Raums der Gitterklassen

Ist $L = Rv + Rw$ ein beliebiges Gitter in $\mathbb{Q}^2$ und ist A eine Matrix in $GL_2(\mathbb{Q})$, so ist auch $A \cdot L = \{A \cdot x : x \in L\}$ ein Gitter. In der mathematischen Fachsprache sagt man: Die Gruppe $GL_2(\mathbb{Q})$ operiert auf der Menge aller Gitter.

Es ist eine gute Übungsaufgabe, sich zu überlegen, dass das Gitter $A \cdot L$ von den beiden Vektoren $A \cdot v$ und $A \cdot w$ erzeugt wird. Ist $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ für eine rationale Zahl a, so entsteht $A \cdot L$ aus L, indem man alle Vektoren in L mit der Zahl a multipliziert. Dieses Gitter nennen wir einfach auch aL.

Ab jetzt betrachten wir statt der Gitter nur noch sogenannte **Gitterklassen**. Wir werden sehen, dass der Raum aller Gitterklassen eine interessante Geometrie besitzt. Hierfür identifizieren wir ab jetzt ein Gitter L mit jedem Gitter aL, so dass a eine beliebige rationale Zahl ist. Wir schreiben $\{L\}$ für die sogenannte Äquivalenzklasse von L, das heißt, $\{L\}$ ist die Menge aller Gitter der Form aL für ein $a \in \mathbb{Q}$. Jedes solche Gitter aL heißt Vertreter der Äquivalenzklasse $\{L\}$. Es ist eine gute Übungsaufgabe, sich zu überlegen, dass $aL = L$ genau dann eintritt, wenn $v_p(a) = 0$ ist. Hier muss man sich kurz daran erinnern, dass R und damit auch unsere Gitter immer von unserer fest gewählten Primzahl p abhängen, die den p-adischen Abstand definiert. Aus dieser Beobachtung folgt $aL = p^{v_p(a)}L$. Die Äquivalenzklasse $\{L\}$ besteht also aus allen „p-Potenz-Vielfachen“ von L.

Mit $X(p)$ bezeichnen wir ab jetzt die Menge aller Äquivalenzklassen von Gittern $\{L\}$.

Die Gruppe $GL_2(\mathbb{Q})$ operiert auch auf der Menge $X(p)$, wenn wir $A\{L\} = \{A \cdot L\}$ setzen. Wir wenden also eine Matrix auf eine Gitterklasse an, indem wir sie auf einen beliebigen Vertreter anwenden.

Wir nennen eine Gitterklasse $\{L\}$ **benachbart** zu einer Gitterklasse $\{M\}$ mit $\{M\} \neq \{L\}$, wenn es einen Vertreter L' von $\{L\}$ (also ein Gitter von der Form $p^m L$) und einen Vertreter M' von $\{M\}$ (also ein Gitter von der Form $p^n M$) gibt, so dass gilt

$$pL' \subset M' \subset L'.$$

Hier ist es sehr günstig, dass wir nicht mit individuellen Gittern, sondern mit Gitterklassen arbeiten. Von einer vernünftigen Nachbarschaftsrelation erwartet man nämlich die Symmetrie, das heißt, es soll gelten: Ist A benachbart zu B, dann ist auch B benachbart zu A. Wenn Sie beispielsweise in der Schule neben Ihrer Banknachbarin sitzen, dann sitzt diese auch neben Ihnen. Ist in der obigen Definition die Gitterklasse $\{L\}$ benachbart zu $\{M\}$, dann gilt $pL' \subset M' \subset L'$ für geeignete Vertreter L' von $\{L\}$ und M' von $\{M\}$. Daraus folgt $pM' \subset pL' \subset M'$, das heißt, die Vertreter M' von $\{M\}$ und pL' von $\{L\}$ erfüllen dieselbe Bedingung mit vertauschten Rollen. Daraus folgt, dass auch $\{M\}$ benachbart zu $\{L\}$ ist.

Jetzt wollen wir uns ein Bild von $X(p)$ machen, indem wir jedes Element von $X(p)$, also jede Gitterklasse, als Punkt darstellen und zwei solche Punkte immer dann durch eine Linie verbinden, wenn die entsprechenden Gitterklassen benachbart sind. Wie sieht dieses Bild von $X(p)$ aus? Mathematisch gesprochen handelt es sich hier um einen **Graphen**, das heißt eine Menge von Punkten (auch Ecken genannt), von denen manche durch Linien (auch Kanten genannt) verbunden sind.

Die folgende Abbildung zeigt drei einfache Beispiele für Graphen.

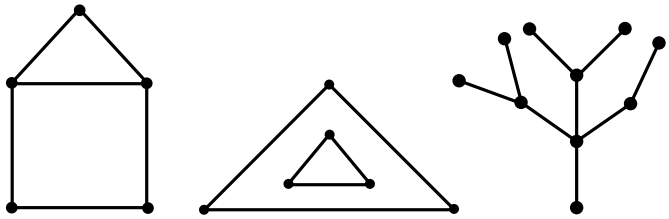

Abbildung 1.2: Drei Graphen

Man nennt eine Folge von Kanten in einem Graphen, die man ohne abzusetzen mit einem Stift nachzeichnen kann, einen **Weg**. Die beiden Graphen links und in der Mitte von Abbildung 1.2 beinhalten **geschlossene Wege**, das heißt, man kann einen „Rundkurs“ einzeichnen, also einen Weg, der in die Anfangsecke zurückführt, ohne dass man dabei einmal auf derselben Kante hin- und gleich wieder zurückläuft. In dem rechten Graphen ist das nicht möglich, er enthält also keinen geschlossenen Weg. Der Graph in der Mitte besteht im Gegensatz zu den beiden äußeren Graphen aus zwei nicht miteinander verbundenen Stücken. Man kann hier keine Ecke in dem äußeren Dreieck mit einer Ecke

in dem inneren Dreieck durch einen Weg verbinden. Der mathematische Fachausdruck hierfür ist, dass der mittlere Graph **unzusammenhängend** ist. Bei den beiden äußeren Graphen ist das anders: Hier kann man von jeder beliebigen Ecke zu jeder beliebigen Ecke einen Weg einzeichnen. Solche Graphen nennen wir **zusammenhängend**.

Definition 1.2 *Ein Graph, der zusammenhängend ist und keine geschlossenen Wege enthält, heißt* **Baum**.

Der rechte Graph in Abbildung 1.2 ist also ein Baum.

Unser Graph $X(p)$ ist allerdings noch etwas komplizierter als die Beispielgraphen in Abbildung 1.2, denn er besteht aus unendlich vielen Ecken (also Gitterklassen). Ist $\{L_0\}$ eine beliebige Gitterklasse mit $L_0 = Rv + Rw$ für zwei Vektoren v und w in $\mathbb{Q}^2$, so liefert die Gitterklasse $L_1 = Rv + R(pw)$ einen Nachbarn von $\{L_0\}$, die Gitterklasse von $L_2 = Rv + R(p^2w)$ liefert einen Nachbarn von $\{L_1\}$ und so weiter. Schauen wir uns negative p-Potenzen an, so liefert $L_{-1} = Rv + Rp^{-1}w$ einen weiteren Nachbarn von $\{L_0\}$ sowie $L_{-2} = Rv + Rp^{-2}w$ einen Nachbarn von $\{L_{-1}\}$, und auch diese Kette können wir immer weiter fortsetzen. Wir werden nun zeigen, dass wir auf diese Weise immer neue Gitterklassen bekommen. Daher bilden die Gitterklassen $\{L_n\}$ zusammen mit ihren Verbindungsstrecken ein Teilstück von $X(p)$, das aussieht wie die an beiden Seiten unendliche Reihe in Abbildung 1.3.

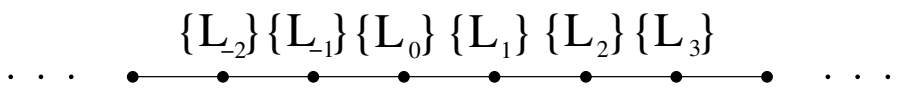

Abbildung 1.3: Ein unendlicher Weg in $X(p)$

Dazu brauchen wir ein paar Vorüberlegungen.

Satz 1.1 *Es seien L und M Gitter in $\mathbb{Q}^2$. Dann gibt es Vektoren v und w in $\mathbb{Q}^2$, die L erzeugen, so dass für geeignete ganze Zahlen m und n die Vektoren $p^m v$ und $p^n w$ das Gitter M erzeugen.*

Beweis: Es gibt Vektoren v' und w' mit $L = Rv' + Rw'$ sowie Vektoren v'' und w'' mit $M = Rv'' + Rw''$. Dabei liegen die beiden Elemente v' und w' der Ebene $\mathbb{Q}^2$ (und auch die beiden Elemente v'' und w'') nicht auf einer gemeinsamen Geraden durch den Nullpunkt. Der mathematische Fachausdruck hierfür ist, dass sie linear unabhängig sind. Daher können wir sowohl v'' als auch w'' in (v', w')-Koordinaten schreiben, wie wir am Ende des Abschnitts 1.2 gesehen haben. Es gilt also

$$v'' = av' + bw' \quad \text{und } w'' = cv' + dw'$$

für geeignete Zahlen a, b, c, d in $\mathbb{Q}$. Nach Definition des Gitters L liegen v'' und w'' genau dann in L, wenn wir die Zahlen a, b, c, d sogar in R wählen können. Das muss im Allgemeinen natürlich nicht der Fall sein.

Vertauschen wir die beiden Vektoren v' und w', so entspricht das der Vertauschung von a mit b und von c mit d. Vertauschen wir die beiden Vektoren v'' und w'', so entspricht das der Vertauschung von a mit c und von b mit d. Nun betrachten wir die Werte $v_p(a), v_p(b), v_p(c)$ und $v_p(d)$, wobei wir vereinbaren, dass $v_p(0) = \infty$ gilt. Wir suchen nun den kleinsten dieser Werte. Ist $v_p(b)$ der kleinste dieser vier Werte, dann vertauschen wir v' und w'. Ist $v_p(c)$ der kleinste dieser vier Werte, dann vertauschen wir v'' und w''. Und ist $v_p(d)$ der kleinste dieser vier Werte, dann vertauschen wir zunächst v' mit w' und danach v'' mit w''. Diese Vertauschung der erzeugenden Vektoren ändert die Gitter nicht. Wir können daher nach eventueller Vertauschung von v mit w und von v' mit w' annehmen, dass $v_p(a)$ höchstens so groß wie jeder der drei anderen Werte $v_p(b), v_p(c)$ und $v_p(d)$ ist. Dann ist automatisch $a \neq 0$, und ferner gilt $v_p(b/a) \geq 0$ und $v_p(c/a) \geq 0$, das heißt, b/a und c/a liegen in R.

Nun setzen wir

$$v = v' + (b/a)w' \text{ und } w = w'.$$

Dann liegt das Gitter $Rv + Rw$ in $L = Rv' + Rw'$. Außerdem gilt $v' = v - (b/a)w$, also liegt L auch in $Rv + Rw$. Daher gilt $L = Rv + Rw$, das heißt, v und w erzeugen das Gitter L.

Ein ähnliches Argument zeigt, dass die Vektoren v'' und $w'' - (c/a)v''$ das Gitter $M = Rv'' + Rw''$ erzeugen. Nun ist

$$v'' = av' + bw' = a\left(v' + \frac{b}{a}w'\right) = av \text{ und } w'' - \frac{c}{a}v'' = \left(d - \frac{bc}{a}\right)w' = \left(d - \frac{bc}{a}\right)w.$$

Da wir hier noch die Faktoren a und $(d - \frac{bc}{a})$ durch p-Potenzen ersetzen können, folgt die Behauptung. □

Wir wenden diesen Satz nun auf zwei Gitter L und M an, deren zugehörige Gitterklassen $\{L\}$ und $\{M\}$ benachbart (also insbesondere verschieden) in $X(p)$ sind. Es gibt daher Vektoren v und w mit $L = Rv + Rw$, so dass $M = Rp^m v + Rp^n w$ für geeignete ganze Zahlen m und n gilt. Gleichzeitig folgt aus der Tatsache, dass $\{L\}$ und $\{M\}$ benachbart sind, dass es einen Vertreter $M' = p^k M$ von $\{M\}$ gibt, der $pL \subset M' \subset L$ erfüllt. (Hier muss man sich als Übungsaufgabe überlegen, dass wir M' so wählen können, dass wir das Gitter L beibehalten können.) Nun ist M' von der Form $M' = Rp^{m+k}v + Rp^{n+k}w$. Aus $M' \subset L$ folgt nun $m+k \geq 0$ und $n+k \geq 0$. Aus $pL \subset M'$ folgt aber auch $m+k \leq 1$ und $n + k \leq 1$. Also können $m + k$ und $n + k$ nur null oder eins sein. Sie können nicht beide gleichzeitig null oder eins sein, denn ansonsten wäre M' äquivalent zu L, und damit wären $\{L\}$ und $\{M\}$ gleich. Also ist eine dieser beiden Zahlen null und die andere eins. Nach eventuellem Vertauschen der Vektoren v und w können wir daher annehmen, dass $M' = Rv + Rpw$ gilt.

Nun können wir die Geometrie des Graphen $X(p)$ studieren.

Satz 1.2 *X(p) ist ein Baum.*

Beweis: Wir müssen nach Definition 1.2 zeigen, dass $X(p)$ zusammenhängend ist und dass $X(p)$ keine geschlossenen Wege enthält.

i) Wir zeigen zunächst, dass $X(p)$ zusammenhängend ist. Dazu betrachten wir zwei Ecken, also Gitterklassen $\{L\}$ und $\{M\}$. Nach Satz 1.1 gibt es Vektoren v und w sowie ganze Zahlen m und n, so dass gilt:

$$L = Rv + Rw \text{ und } M = Rp^m v + Rp^n w.$$

Indem wir gegebenenfalls die Vektoren v und w vertauschen, können wir annehmen, dass $m \leq n$, also $n - m \geq 0$ ist. Da das Gitter $M' = p^{-m}M = Rv + Rp^{n-m}w$ äquivalent zu M ist, gilt $\{M\} = \{M'\}$. Wir können also mit M' weiterarbeiten. Nun betrachten wir die Gitterklassen zu den Gittern $L = Rv + Rw$, $Rv + Rpw$, $Rv + Rp^2w$ bis hin zu $Rv + Rp^{n-m}w$. Sie bilden einen Weg von $\{L\}$ nach $\{M'\}$.

Daher sind zwei beliebige Ecken in $X(p)$ duch einen Weg verbunden, das heißt, $X(p)$ ist zusammenhängend.

ii) Nun wollen wir noch zeigen, dass $X(p)$ keine geschlossenen Wege enthält. Wir beschränken uns hier darauf, nachzuweisen, dass $X(p)$ keine Dreiecke enthält. Unter einem Dreieck verstehen wir einen geschlossenen Weg, der aus drei verschiedenen Kanten besteht, die drei Ecken $\{L\}$, $\{M\}$ und $\{N\}$ verbinden. Diese sind dann paarweise zueinander benachbart und bilden somit einen Teil von $X(p)$, der wie ein Dreieck aussieht. Angenommen, die Ecken $\{L\}$, $\{M\}$ und $\{N\}$ bilden solch ein Dreieck. Wir werden zeigen, dass dies zu einem Widerspruch führt. Wir wenden nun die Überlegungen im Anschluss an Satz 1.1 auf die benachbarten Gitterklassen $\{L\}$ und $\{M\}$ an. Also gibt es (eventuell nach Übergang zu anderen Vertretern dieser Gitterklassen) Vektoren v und w mit $L = Rv + Rw$ und $M = Rv + Rpw$. Da $\{L\}$ und $\{N\}$ benachbart sind, können wir, indem wir eventuell N durch eine äquivalente Gitterklasse ersetzen, annehmen, dass

$$pL \subset N \subset L.$$

Ferner sind M und N benachbart. Daher gibt es eine ganze Zahl k, so dass

$$p^{k+1}N \subset M \subset p^k N$$

gilt.

Aus $v \in M \subset p^k N \subset p^k L = Rp^k v + Rp^k w$ folgt, dass $k \leq 0$ sein muss. Aus $pw \in pL \subset N \subset p^{-(k+1)}M = Rp^{-(k+1)}v + Rp^{-(k+1)}(pw)$ folgt, dass $k+1 \geq 0$, also $k \geq -1$ ist. Daher ist k entweder gleich 0 oder gleich -1.

1. Fall $k = 0$**:** In diesem Fall gilt $pN \subset M \subset N$. Wir wissen, dass M nicht gleich N ist, denn die zugehörigen Gitterklassen sind benachbart, also insbesondere verschieden. Wir betrachten ein Element aus N, das nicht in M liegt. Da N in $L = Rv+Rw$ enthalten ist, können wir es als $av + bw$ mit a und b in R schreiben. Nun liegen v und pw in M. Da $av + bw$ nicht in M enthalten ist, muss $v_p(b) = 0$ sein. Da aber v in M und damit in

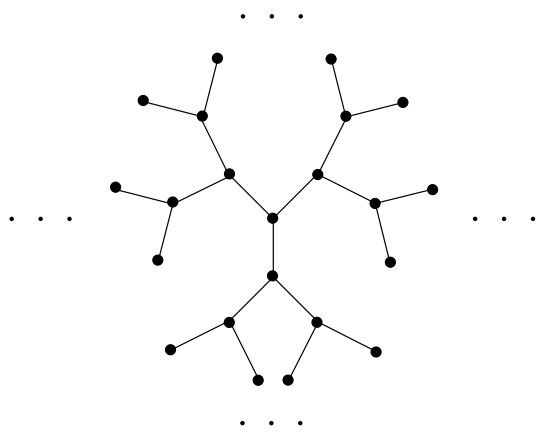

Abbildung 1.4: Der Baum $X(2)$

N liegt, gehört auch av zu N und damit auch bw, denn es gilt $bw = av + bw - av$. Da $v_p(b) = 0$ ist, liegt die rationale Zahl $1/b$ ebenfalls in R, das heißt, $w = (1/b)bw$ ist in N enthalten. Aber dann haben wir gezeigt, dass v und w und damit ganz L in N enthalten ist. Da wir $N \subset L$ bereits wissen, folgt hieraus $L = N$. Das kann aber nicht sein, denn die Gitterklassen $\{L\}$ und $\{N\}$ sind benachbart, also insbesondere verschieden. Wir sind hier also auf einen Widerspruch gestoßen.

2. Fall $k = -1$**:** In diesem Fall gilt $N \subset M \subset p^{-1}N$. Wir betrachten die Inklusion $pL \subset N \subset L$ und argumentieren ähnlich wie im ersten Fall. Da $pL \neq N$ ist, gibt es ein Element in N, das nicht in pL liegt. Da N in $M = Rv + Rpw$ enthalten ist, können wir dieses Element als $av + bpw$ mit a und b in R schreiben. Da pw in pL und damit in N enthalten ist, gehört auch bpw zu N, und damit liegt auch $av = av + bpw - bpw$ in N. Da wir angenommen haben, dass $av + bpw$ nicht in pL liegt, folgt $v_p(a) = 0$. Also ist auch $1/a$ in R enthalten, das heißt, $v = (1/a)av$ liegt in N. Aber dann haben wir gezeigt, dass v und pw und damit ganz M in N enthalten ist. Da wir $N \subset M$ bereits wissen, folgt hieraus $M = N$, was im Widerspruch dazu steht, dass $\{M\}$ und $\{N\}$ benachbart, also inbesondere verschieden sind.

In beiden Fällen erhalten wir also einen Widerspruch. Daher muss unsere Annahme falsch sein, und es kann kein Dreieck in $X(p)$ geben. Mit ähnlichen Argumenten kann man zeigen, dass $X(p)$ auch keine geschlossenen Wege größerer Länge enthält. Wir verzichten hier allerdings auf weitere Details. Ein vollständiger Beweis ist in Kapitel II, §1 des Buches [Se] zu finden. □

Man kann sogar beweisen, dass $X(p)$ ein sogenannter $(p+1)$-regulärer Baum ist, das heißt, in jeder Ecke von $X(p)$ zweigen genau $p + 1$ Kanten ab. Abbildung 1.4 stellt den unendlichen Baum $X(2)$ dar, wobei die Pünktchen andeuten, dass er sich in alle Richtungen immer weiter fortsetzt.

1.4 Ausblick

Wie wir oben schon gesehen haben, ist für jede Gitterklasse $\{L\}$ und jede Matrix A in $GL_2(\mathbb{Q})$ auch $\{A \cdot L\}$ eine Gitterklasse. Es ist nicht schwierig, sich zu überlegen, dass mit $\{L\}$ und $\{M\}$ auch $\{A \cdot L\}$ und $\{A \cdot M\}$ benachbart sind. Also bildet die Matrix A Ecken des Graphen $X(p)$ auf Ecken und Kanten des Graphen $X(p)$ auf Kanten ab.

Um die Struktur von Gruppen zu studieren, ist es oft sehr hilfreich, sie auf einem geometrischen Objekt operieren zu lassen.

So verrät auch die Operation der Gruppe $SL_2(\mathbb{Q})$ auf dem Baum $X(p)$ einiges über ihre Struktur. Wir betrachten zum Beispiel beschränkte Untergruppen von $SL_2(\mathbb{Q})$. Das sind Teilmengen von $SL_2(\mathbb{Q})$, die selbst eine Gruppe unter der Matrixmultiplikation bilden und die zusätzlich die Eigenschaft haben, dass es eine Schranke C gibt, so dass alle Einträge aller Matrizen in der Teilmenge höchstens den p-adischen Abstand C vom Nullpunkt haben. Die Gruppe $SL_2(\mathbb{Q})$ selbst ist offenbar nicht beschränkt, denn man kann Matrizen der Determinante eins hinschreiben, in denen ein Eintrag beliebig groß wird (versuchen Sie es einmal). Nun kann man zeigen, dass eine Untergruppe von $SL_2(\mathbb{Q})$ genau dann beschränkt ist, wenn es eine Ecke in $X(p)$ gibt, die von allen ihren Elementen festgehalten wird. Dies hat wiederum interessante gruppentheoretische Konsequenzen für die Struktur dieser Untergruppe.

Das Zusammenspiel von Geometrie, Gruppentheorie und der p-adischen Welt hat viele faszinierende Aspekte. Von einem höheren mathematischen Standpunkt aus ist der Baum $X(p)$ ein Beispiel eines sogenannten „Bruhat-Tits-Gebäudes“. Solche Gebäude kann man auch für andere Matrixgruppen in der p-adischen Welt definieren. Sie sind in der Regel von höherer Dimension als der Baum und daher nicht mehr gut zu zeichnen. Trotzdem haben Mathematikerinnen und Mathematiker viele spannende Ergebnisse über diese Objekte herausgefunden.

Literaturverzeichnis

Das Buch [Gou] bietet eine ausführliche Einführung in die p-adische Welt, die für Studienanfänger geeignet ist. In dem grundlegenden Werk [Se] wird das faszinierende Zusammenspiel von Gruppen und Bäumen erklärt. Dieses Buch ist allerdings recht dicht geschrieben und erfordert etwas Erfahrung im Umgang mit mathematischen Texten.

[Gou] Fernando Q. Gouvea: p-adic Numbers. An introduction. Springer Verlag 2003.

[Se] Jean-Pierre Serre: Trees. Springer Verlag 1980.