Prof. Dr. H. Brenner **Osnabrück WS 2020/2021**

Algebraische Zahlentheorie

Vorlesung 1

Wir besprechen einige typische Situation, die zur algebraischen Zahlentheorie führen.

Primfaktorzerlegung in $\mathbb{Z}$ und sonstwo

In den ganzen Zahlen $\mathbb{Z}$ gilt die eindeutige Primfaktorzerlegung, d.h. jede ganze Zahl $n \neq 0$ lässt sich als ein (bei einer negativen Zahl braucht man noch das Vorzeichen -1) Produkt von (positiven) Primzahlen schreiben, wobei die Anzahl der auftretenden Primzahlen, die Primfaktoren, eindeutig bestimmt ist. Beispielsweise ist

$$175 = 5 \cdot 5 \cdot 7 = 5 \cdot 7 \cdot 5 = 5^2 \cdot 7.$$

Für eine Primzahl ist diese Faktorzerlegung einfach die Zahl selbst. In einem größeren Ring, beispielsweise einem Körper, ergeben sich neue Darstellungsmöglichkeiten. Es ist in $\mathbb{R}$

$$7 = \frac{7}{5} \cdot 5 = 7 \cdot 5^{-1} \cdot 5 = 7 \cdot \pi^{-1}\pi.$$

Das sind natürlich Uneindeutigkeiten, die sich einfach daraus ergeben, dass es Elemente gibt, die ein Inverses besitzen. Wenn man an $7 = (-1)(-7)$ denkt, gibt es dieses Phänomen schon in $\mathbb{Z}$. Wir halten kurz die folgende Definition fest.

Definition 1.1. Ein Element u in einem kommutativen Ring R heißt *Einheit*, wenn es ein Element $v \in R$ mit $uv = 1$ gibt.

In $\mathbb{Z}$ sind nur 1 und -1 Einheiten, der Einfluss auf die Teilbarkeitstheorie ist daher sehr überschaubar. Ein kommutativer Ring ist genau dann ein Körper, wenn in ihm jedes von 0 verschiedene Element eine Einheit ist (der Nullring ist kein Körper, da in ihm sogar die 0 eine Einheit ist). Deshalb gibt es in einem Körper keine aussagekräftige Teilbarkeitstheorie. Ein anderes Phänomen sind die Faktorzerlegungen

$$7 = \sqrt{7} \cdot \sqrt{7} = \sqrt[3]{7} \cdot \sqrt[3]{7} \cdot \sqrt[3]{7} = \sqrt[4]{7} \cdot \sqrt[4]{7} \cdot \sqrt[4]{7} \cdot \sqrt[4]{7}.$$

In diesem Sinne kann man beliebig weitermachen, es gibt dann für die Zahl 7 beliebig lange zunehmend feinere Zerlegungen - aber keine Primfaktorzerlegung.

Betrachten wir genauer die Zerlegung

$$7 = \sqrt{7} \cdot \sqrt{7}.$$

Diese hat nichts mit Einheiten zu tun, sondern allein mit der Existenz der Quadratwurzel (oder in den weiteren Fällen mit der Existenz der dritten oder vierten Wurzel) der 7. Um eine solche Faktorzerlegung hinzuschreiben, braucht man nicht die vollen reellen Zahlen, sondern eben nur diese Wurzeln. Um die erste Gleichung ausdrücken zu können, braucht man nur das neue Element $\sqrt{7}$ mit der charakteristischen Eigenschaft, dass das Produkt mit sich selbst gleich 7 ist. Doch allein diese Hinzunahme, also die Mengen $\mathbb{N} \cup \{\sqrt{7}\}$ bzw. $\mathbb{Z} \cup \{\pm\sqrt{7}\}$ liefert keine sinnvolle algebraische Struktur, da darin weder die Multiplikation $4 \cdot \sqrt{7}$ noch die Addition $4 + \sqrt{7}$ definiert ist. Da verliert man also viel zu viel. Man möchte „nur“ die Quadratwurzel aus 7 hinzutun, aber gleichzeitig sinnvolle algebraische Strukturen erhalten. Mit $\sqrt{7}$ muss dann auch beispielsweise $13 - 22\sqrt{7}$ drin sein. Zahlen von dieser Form sind offenbar additiv abgeschlossen und sind aber auch multiplikativ abgeschlossen, es gilt ja

$$\left(a + b\sqrt{7}\right)\left(c + d\sqrt{7}\right) \ = \ (ac + 7bd) + (ad + bc)\sqrt{7}$$

für beliebige $a, b, c, d \in \mathbb{Z}$. Diese Zahlen bilden also wieder einen kommutativen Ring, und zwar kann man ihn als Unterring der reellen Zahlen realisieren, weshalb die Assoziativität der Verknüpfungen direkt erfüllt ist. Wir haben also eine Ringerweiterung

$$\mathbb{Z} \ \subseteq \ \mathbb{Z}[\sqrt{7}] \ = \ \mathbb{Z} + \mathbb{Z}\sqrt{7} \ = \ \left\{a + b\sqrt{7} \mid a, b \in \mathbb{Z}\right\} \ =: \ R,$$

wobei die ganzen Zahlen den Summen $a + b\sqrt{7}$ mit $b \ = \ 0$ entsprechen, wobei die Addition in R komponentenweise und die Multiplikation wie in $\mathbb{R}$ bzw. explizit wie oben bzw. distributiv unter Verwendung der einzigen relevanten Regel

$$\sqrt{7} \cdot \sqrt{7} \ = \ 7$$

erklärt ist. Die Darstellung $a + b\sqrt{7}$ eines Elementes aus R ist ferner eindeutig, d.h. $a + b\sqrt{7} \ = \ a' + b'\sqrt{7}$ ist nur bei

$$a \ = \ a'$$

und

$$b \ = \ b'$$

möglich. Anderfalls hätte man eine Gleichung

$$r \ = \ s\sqrt{7}$$

mit $r, s \in \mathbb{Z} \ \ r, s \neq 0$, woraus sich

$$\sqrt{7} \ = \ \frac{r}{s}$$

im Widerspruch zur Irrationalität von Quadratwurzeln auf Primzahlen ergibt, die aus der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ folgt, siehe Aufgabe 1.2. (der Spezialfall, die Irrationalität der Quadratwurzel aus 2, ist ein typisches Beispiel für einen Widerspruchsbeweis aus den Anfängervorlesungen, siehe Satz 4.6 (Mathematik für Anwender (Osnabrück 2020-2021))).

Aufgrund der definierenden Gleichung sieht man direkt, dass 7 in R nicht mehr prim ist, sondern nichttriviale Teiler, nämlich $\sqrt{7}$ besitzt, wobei wir aber die exakten Definitionen noch nicht fixiert haben. Zunächst muss man sich klar machen, dass 7 (und $\sqrt{7}$) keine Einheit in R wird. Dies kann man aber wegen

$$7(a+b\sqrt{7}) \;=\; 7a+7b\sqrt{7} \;=\; 1$$

sofort ausschließen. Was aber keineswegs klar ist, ob es in R weitere Faktorzerlegungen für 7 gibt, ob $\sqrt{7}$ prim ist, ob es neue Einheiten in R gibt, wie sich die Existenz von $\sqrt{7}$ auf die Faktorzerlegung von anderen ganzen Zahlen auswirkt. Um Zerlegungsphänome von der Bauart

$$7 \;=\; u(u^{-1}7)$$

mit einer Einheit u auszuschließen bzw. zu erkennen, müssen wir zuerst wissen, ob in R neue Einheiten dazukommen. Mit dem Argument von eben kann man direkt einsehen, dass ganze Zahlen $\neq 1,-1$ in R Nichteinheiten bleiben. Es gibt aber in der Tat eine Vielzahl von neuen Einheiten! Betrachten wir in R die Gleichung

$$(8+3\sqrt{7})(8-3\sqrt{7}) \;=\; 64-9\cdot 7 \;=\; 1,$$

die ja besagt, dass die beiden Elemente $8+3\sqrt{7}$ und $8-3\sqrt{7}$ zueinander invers sind und damit Einheiten sind. Damit sind auch alle Zahlen der Form $\pm\big(8+3\sqrt{7}\big)^n$ (mit $n\in\mathbb{Z}$) Einheiten, und das sind alle Einheiten von R, siehe die 25. Vorlesung. Die Existenz von Einheiten erschwert die Entscheidung, ob eine Faktorzerlegung auf Einheiten beruht oder auf eine Zerlegung in substantiell grundlegendere Bestandteile. Handelt es sich beispielsweise bei

$$(5+4\sqrt{7})(-5+4\sqrt{7}) \;=\; -25+16\cdot 7 \;=\; -25+112 \;=\; 87 \;=\; 3\cdot 29$$

um zwei wesentlich verschiedene Faktorzerlegungen der 87 in R? Hier haben wir schon zum zweiten Mal die dritte binomische Formel ausgenutzt, um durch eine Multiplikation von zwei Zahlen aus R wieder in $\mathbb{Z}$ zu landen. Wegen

$$3 \;=\; (2+\sqrt{7})(-2+\sqrt{7})$$

kann man aber die 3 weiter zerlegen. Der erste Faktor kommt auch in der Zerlegung

$$5+4\sqrt{7} \;=\; (2+\sqrt{7})(6-\sqrt{7})$$

vor. In der verfeinerten Zerlegung

$$87 \;=\; (2+\sqrt{7})(-2+\sqrt{7})(6-\sqrt{7})(6+\sqrt{7})$$

kommen somit beide obigen Zerlegungen vor, die sich daher als keine Primfaktorzerlegung erweisen. Das ist also wie bei

$$210 \;=\; 6\cdot 35 \;=\; 10\cdot 21 \;=\; 2\cdot 3\cdot 5\cdot 7,$$

allerdings mit dem Unterschied, dass es in R zunächst einmal keine systematische Methode gibt, Zahlen auf die Primeigenschaft zu überprüfen.

Eine wichtige Fragestellung der algebraischen Zahlentheorie ist, wie sich Teilereigenschaften und die Primfaktorzerlegungen von $\mathbb{Z}$ ändern, wenn man zusätzliche Elemente hinzunimmt. Typischerweise werden dabei die Primfaktorzerlegungen zerstört, es entstehen aber neue Faktorzerlegungen (nicht unbedingt Primfaktorzerlegungen), die selbst wieder zahlentheoretischen Sachverhalte ausdrücken und sichtbar machen.

Summe von Quadraten

Betrachten wir die Frage, welche natürlichen Zahlen die Summe von zwei Quadratzahlen sind. Anders formuliert, für welche n hat die Gleichung

$$n = x^2 + y^2$$

Lösungen mit ganzen Zahlen x, y? Es ist

$$0 = 0 + 0$$
$$1 = 1 + 0$$
$$2 = 1 + 1$$
$$3$$

$$4 = 4 + 0$$

$$5 = 4 + 1$$
$$6$$

$$7$$

$$8 = 4 + 4$$
$$9 = 9 + 0$$
$$10 = 9 + 1$$
$$11$$

$$12$$

$$13 = 9 + 4$$
$$14$$

$$15$$

$$16 = 16 + 0$$

$$17 = 16 + 1$$
$$18 = 9 + 9$$
$$19$$

$$20 = 16 + 4$$
$$21$$

Erkennt man hier schon eine Struktur? Es ist in der Zahlentheorie üblich, solche Fragen erst einmal für Primzahlen zu verstehen, und die Ergebnisse dann auf zusammengesetzte Zahlen zu übertragen. Von den Primzahlen ≤ 20 sind $3, 7, 11, 19$ keine Summe von zwei Quadraten, während $2, 5, 13$ und 17 es sind. Es fällt auf, dass die erste Reihe alle den Rest 3 bei Division durch 4 haben, und die zweite Reihe (von 2 abgesehen) den Rest 1. Hier zeigt sich, dass es sinnvoll ist, zu anderen, hier endlichen, Ringen überzugehen, um Fragen über natürliche oder ganze Zahlen zu beantworten. Die Restabbildung zur *Division mit Rest* durch 4 ist ein Ringhomomorphismus

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(4) = \{0, 1, 2, 3\},\ n \longmapsto n \mod 4.$$

Dabei ist in $\mathbb{Z}/(4)$ die Addition und die Multiplikation modulo 4 erklärt, also etwa $3 \cdot 3 = 9 = 1$. Die Abbildung respektiert also die Addition und die Multiplikation. Wenn nun die Gleichung

$$n = x^2 + y^2$$

in $\mathbb{Z}$ eine Lösung besitzt, so liefert das sofort auch eine Lösung modulo 4, nämlich

$$n = x^2 + y^2 \mod 4$$

bzw.

$$(n \mod 4) = (x \mod 4)^2 + (y \mod 4)^2$$

oder

$$\bar{n} = \bar{x}^2 + \bar{y}^2.$$

Nun sind aber in $\mathbb{Z}/(4)$ die Quadrate einfach

$$0^2 = 2^2 = 0$$

und

$$1^2 = 3^2 = 1$$

und damit sind $0, 1$ und 2 Summen von zwei Quadraten in $\mathbb{Z}/(4)$, aber nicht 3. Es bestätigt sich also bereits die obige Beobachtung, dass natürliche Zahlen (nicht nur Primzahlen), die den Rest 3 modulo 4 haben, nicht die Summe von zwei Quadraten sein können.

Für Primzahlen mit dem Rest 1 modulo 4 liefert die Betrachtung im Restklassenring $\mathbb{Z}/(4)$ natürlich nur, dass eine notwendige Bedingung erfüllt ist, woraus sich natürlich noch lange nicht auf eine Darstellung als Summe von zwei Quadraten schließen lässt. Die Zahl 21 zeigt auch, dass eine Zahl, die

modulo 4 den Rest 1 besitzt, nicht notwendig selbst die Summe von zwei Quadraten ist.

Eine wichtige Umformulierung der Frage erhält man, wenn man wie oben zu einer quadratischen Erweiterung übergeht, nämlich zum *Ring der Gaußschen Zahlen*

$$\mathbb{Z}[\mathrm{i}] \;=\; \mathbb{Z} \oplus \mathbb{Z}\mathrm{i}$$

(einem Unterring der komplexen Zahlen). Dort können wir

$$n \;=\; x^2 + y^2 \;=\; (x + \mathrm{i}y)(x - \mathrm{i}y)$$

schreiben, wodurch die Frage, ob eine Zahl Summe von zwei Quadraten ist, mit der Frage der multiplikativen Zerlegung von natürlichen Zahlen in diesem neuen Ring in Zusammenhang gebracht wird. Insbesondere ist eine Primzahl, die Summe von zwei Quadraten ist, im Ring der Gaußschen Zahlen nicht mehr prim (die hingeschriebenen Faktoren können keine Einheiten sein).

Die Frage nach den Summen von zwei Quadraten werden wir abschliesend in Satz 9.11 beantworten.

Pellsche Gleichung

Betrachten wir eine Zahlbereichserweiterung

$$\mathbb{Z} \;=\; \mathbb{Z}[\sqrt{D}] \;=\; \mathbb{Z} \oplus \mathbb{Z}\sqrt{D}$$

mit einer ganzen Zahl D, die beiden Fälle $D = 7$ und $D = -1$ haben wir schon etwas genauer in den Blick genommen (es sei D quadratfrei, enthalte also keinen Primfaktor mehrfach). Auch der Frage, wie in diesen Ringen die Einheiten aussehen, sind wir schon begegnet. Betrachten wir allgemein die Bedingung, ob es zu $a + b\sqrt{D}$ ein Element $c + e\sqrt{D}$ mit

$$\left(a + b\sqrt{D}\right)\left(c + e\sqrt{D}\right) \;=\; 1.$$

Wenn a und b nicht teilerfremd sind, so kann es keine Lösung geben, seien also a und b teilerfremd. Dann folgt aus

$$bc + ae \;=\; 0,$$

dass bis auf einen gemeinsamen Vorfaktor

$$c \;=\; fa$$

und

$$e \;=\; -fb$$

gilt, und der Vorfaktor muss 1 oder -1 sein. Die Frage nach den Einheiten ist also im Wesentlichen die Frage, ob

$$\left(a + b\sqrt{D}\right)\left(a - b\sqrt{D}\right) \;=\; a^2 - b^2 D \;=\; \pm 1.$$

Es geht also darum, welche ganzzahligen Lösungen bei gegebenem D die Gleichung

$$x^2 - y^2 D = \pm 1$$

besitzt. Man spricht von der *Pellschen Gleichung*, deren Lösungsverhalten wesentlich von D positiv oder negativ abhängt.

Diophantische Gleichungen

Eine besondere Herausforderung innerhalb der Zahlentheorie sind diophantische Gleichungen.

Definition 1.2. Zu einem Polynom $F \in \mathbb{Z}[x_1, \ldots, x_n]$ heißt

$$F(x_1, \ldots, x_n) = 0$$

eine *diophantische Gleichung*. Unter einer Lösung einer diophantischen Gleichung versteht man ein ganzzahliges Zahlentupel $(x_1, \ldots, x_n) \in \mathbb{Z}^n$, das in F eingesetzt 0 ergibt.

Die Pellsche Gleichung haben wir schon erwähnt, bei linearen diophantischen Gleichungen ist das Lösungsverhalten einfach zu verstehen, die Gleichung

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

ist die Frage nach *Pythagoreischen Tripeln*, was ebenfalls gut verstanden ist. Eine wesentliche Frage bei diophantischen Gleichungen ist, ob es überhaupt, eventuell abgesehen von trivialen Lösungen, ganzzahlige Lösungen gibt. Ein weiteres wichtiges Problem ist, ob es endlich viele oder unendlich viele ganzzahlige Lösungen gibt. Ein großes zahlentheoretisches Problem, das erst 1995 gelöst wurde, ist das Problem von Fermat, ob die Gleichung

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

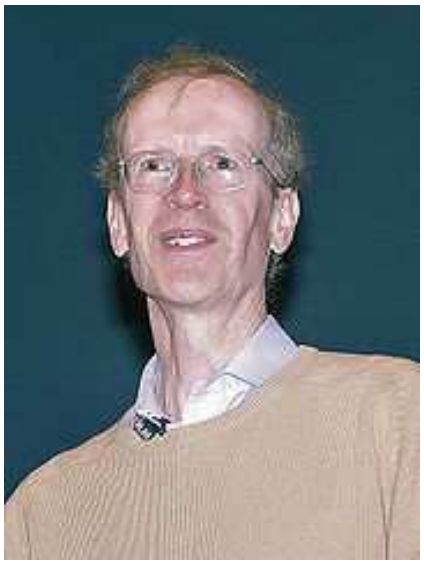
mit $n \geq 3$ nichttriviale ganzzahlige Lösungen (x, y, z) besitzt, in denen alle Einträge nicht 0 sind.

Satz 1.3. *Die diophantische Gleichung*

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

besitzt für kein $n \geq 3$ eine ganzzahlige nichttriviale Lösung.

Beweis. Der Beweis für diese Aussage geht bei Weitem über den Inhalt einer Vorlesung über elementare oder algebraische Zahlentheorie hinaus. □



Andrew Wiles (*1953)

Der Beweis für diesen Satz verwendet die reichhaltige Theorie der elliptischen Kurven. Vor diesem Beweis wurden die besten Resultate zu diesem Problem mit Methoden der algebraischen Zahlentheorie erzielt, und zwar konnten sehr viele Exponenten erledigt werden. Die Grundidee geht folgendermaßen: Die Fermat-Gleichung erhält einen neuartigen Charakter, wenn man sie in dem Ring betrachten, der aus $\mathbb{Z}$ entsteht, wenn man eine n-te Einheitswurzel ζ hinzunimmt. Das ist eine Zahl, deren n-te Potenz 1 ist. Solche Einheitswurzeln gibt es innerhalb der komplexen Zahlen, beispielsweise ist $e^{2\pi \mathrm{i}/n}$ eine primitive n-te Einheitswurzel. Wichtig sind hier aber die algebraischen Eigenschaften. Jedenfalls kann man die etwas umgeschriebene Fermatgleichung

$$x^n - z^n = -y^n$$

unter Verwendung einer primitiven Einheitswurzel als

$$x^n - z^n = (x-z)(x-\zeta z)\cdots(x-\zeta^{n-1}z) = -y^n$$

schreiben. Somit hat man zwei ziemlich verschiedene Faktorzerlegungen einer Zahl. Wenn man jetzt noch was weiß, dass in diesem neuen Ring die eindeutige Primfaktorzerlegung gilt, so kann man (das sind dann immer noch mehrere Schritte) daraus einen Widerspruch ableiten. An dieser STelle gibt es eine schlechte und eine gute Nachricht: Diese Ringe besitzen häufig nicht die eindeutige Primfaktorzerlegung, das angedeutete Argument funktioniert aber auch noch dann, wenn man weiß, dass die sogenannte Klassengruppe des Ringes eine gewisse Eigenschaft erfüllt, die deutlich schwächer als die eindeutige Primfaktorzerlegung ist.

Für $n = 4$ ist die imaginäre Einheit i eine vierte primitive Einheitswurzel (wegen $\mathrm{i}^4 = 1$), in diesem Fall gilt

$$y^4 - z^4 = (x-z)(x-\mathrm{i}z)(x+z)(x+\mathrm{i}z) = -y^4$$

und man kann die Situation im Ring der Gaußschen Zahlen $\mathbb{Z}[i]$ analysieren.

Beispiel 1.4. Als Kuriosität erwähnen wir, dass die von Euler vermutete teilweise Verallgemeinerung des Fermatschen Problems, dass die Gleichungen

$$x^4 + y^4 + z^4 = u^4,$$
$$x^5 + y^5 + z^5 + u^5 = v^5,$$

usw. keine ganzzahlige Lösung besitzen, also dass zwischen n n-ten Potenzen keine additive Beziehung bestehen kann, nicht gilt. Die einfachsten Gegenbeispiele sind

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

und

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

Abbildungsverzeichnis