Prof. Dr. H. Brenner **Osnabrück WS 2016/2017**

Zahlentheorie

Vorlesung 1

In der Zahlentheorie wollen wir Eigenschaften der ganzen Zahlen verstehen. Dazu ist es sinnvoll, nicht nur $\mathbb{Z}$ selbst zu betrachten, sondern auch davon abgeleitete Objekte, wie Restklassenringe (Modulare Arithmetik), Ringe der ganzen Zahlen in Körpererweiterungen von $\mathbb{Q}$, wie etwa den Ring der Gaussschen Zahlen, Lokalisierungen und Komplettierungen wie die p-adischen Zahlen. Die grundlegende Gemeinsamkeit dieser Objekte ist, dass es sich um kommutative Ringe handelt. Deshalb werden wir von Anfang an die benötigten Begriffe auf der Ringebene entwickeln.

Beispiel 1.1. 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

$$0 = 0 + 0$$

$$1 = 1 + 0$$

$$2 = 1 + 1$$

$$3$$

$$4 = 4 + 0$$

$$5 = 4 + 1$$

$$6$$

$$7$$

$$8 = 4 + 4$$

$$9 = 9 + 0$$

$$10 = 9 + 1$$

$$11$$

$$12$$

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

$$15$$

$$16 = 16 + 0$$
$$17 = 16 + 1$$
$$18 = 9 + 9$$
$$19$$

$$20 = 16 + 4$$

Erkennt man hier schon eine Struktur? Es ist in der Zahlentheorie üblich, solche Fragen erstmal 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 bereits, dass es sinnvoll ist, zu anderen Ringen überzugehen, um Fragen über natürliche 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 Summe von 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. Wir werden aber im Verlauf der Vorlesung sehen, dass es für Primzahlen mit dieser Restbedingung gilt. Dafür werden wir in einem weiteren Ring arbeiten, nämlich im *Ring der Gaußschen Zahlen*

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

(einem Unterring der komplexen Zahlen). Dort können wir schreiben

$$n = x^2 + y^2 = (x + iy)(x - iy),$$

wodurch die Frage, ob eine Zahl Summe von zwei Quadraten ist, mit der Frage der multiplikativen Zerlegung von natürlichen Zahlen in einem neuen Ring in Zusammenhang gebracht wird.

Die Frage nach den Summen von zwei Quadraten werden wir abschliesend in Satz 9.10 beantworten.

Wir erinnern kurz an die Definition eines Ringes und eines kommutativen Ringes.

Definition 1.2. Ein *Ring* R ist eine Menge mit zwei Verknüpfungen $+$ und $\cdot$ und mit zwei ausgezeichneten Elementen 0 und 1 derart, dass folgende Bedingungen erfüllt sind:

(1) $(R, +, 0)$ ist eine abelsche Gruppe.
(2) $(R, \cdot, 1)$ ist ein Monoid.
(3) Es gelten die *Distributivgesetze*, also $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ für alle $a, b, c \in R$.

Definition 1.3. Ein Ring R heißt *kommutativ*, wenn die Multiplikation kommutativ ist.

Das wichtigste Beispiel für uns ist der (kommutative) Ring der ganzen Zahlen $\mathbb{Z}$. Wir werden aber noch viele weitere Ringe kennenlernen, die zahlentheoretisch relevant sind. Wir verwenden wie üblich die Konvention, dass die Multiplikation stärker bindet als die Addition und schreiben in der Regel ab anstatt $a \cdot b$.

Oben hatten wir im Zusammenhang mit der Abbildung $\mathbb{Z} \to \mathbb{Z}/(4)$ den Begriff Ringhomomorphismus erwähnt, den wir hier kurz anführen.

Definition 1.4. Seien R und S Ringe. Eine Abbildung

$$\varphi\colon R \longrightarrow S$$

heißt *Ringhomomorphismus*, wenn folgende Eigenschaften gelten:

(1) $\varphi(a+b) = \varphi(a) + \varphi(b)$
(2) $\varphi(1) = 1$
(3) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Teilbarkeitsbegriffe

DEFINITION 1.5. Sei R ein kommutativer Ring, und a, b Elemente in R. Man sagt, dass a das Element b *teilt* (oder dass b von a geteilt wird, oder dass b ein *Vielfaches* von a ist), wenn es ein $c \in R$ derart gibt, dass $b = c \cdot a$ ist. Man schreibt dafür auch $a|b$.

LEMMA 1.6. *In einem kommutativen Ring R gelten folgende Teilbarkeitsbeziehungen.*

(1) *Für jedes Element a gilt $1 \mid a$ und $a \mid a$.*
(2) *Für jedes Element a gilt $a \mid 0$.*
(3) *Gilt $a \mid b$ und $b \mid c$, so gilt auch $a \mid c$.*
(4) *Gilt $a \mid b$ und $c \mid d$, so gilt auch $ac \mid bd$.*
(5) *Gilt $a \mid b$, so gilt auch $ac \mid bc$ für jedes $c \in R$.*
(6) *Gilt $a \mid b$ und $a \mid c$, so gilt auch $a \mid rb+sc$ für beliebige Elemente $r, s \in R$.*

Beweis. Siehe Aufgabe 1.21. □

DEFINITION 1.7. Ein Element u in einem kommutativen Ring R heißt *Einheit*, wenn es ein Element $v \in R$ mit $uv = 1$ gibt.

BEMERKUNG 1.8. Eine Einheit ist also ein Element, das die 1 teilt. Das Element v mit der Eigenschaft $uv = 1$ ist dabei eindeutig bestimmt. Hat nämlich auch w die Eigenschaft $uw = 1$, so ist

$$v = v1 = v(uw) = (vu)w = 1w = w.$$

Das im Falle der Existenz eindeutig bestimmte v mit $uv = 1$ nennt man das (multiplikativ) *Inverse* zu u und bezeichnet es mit u^{-1}. Die Menge aller Einheiten in einem kommutativen Ring bilden eine kommutative Gruppe (bezüglich der Multiplikation mit 1 als neutralem Element), die man die *Einheitengruppe* von R nennt. Sie wird mit $R^\times$ bezeichnet.

In den Ringen, die uns bisher begegnet sind, sind die Einheitengruppen einfach zu bestimmen. Es ist $\mathbb{Z}^\times = \{1, -1\}$ und $(\mathbb{Z}/(4))^\times = \{1, 3\}$. Im Ring der Gaußschen Zahlen gibt es vier Einheiten: $1, -1, i, -i$, siehe die nächste Vorlesung.

DEFINITION 1.9. Zwei Elemente a und b eines kommutativen Ringes R heißen *assoziiert*, wenn es eine Einheit $u \in R$ derart gibt, dass $a = ub$ ist.

Bemerkung 1.10. Die Assoziiertheit ist eine Äquivalenzrelation. Siehe Aufgabe 1.7.

Das folgende Lemma besagt, dass es für die Teilbarkeitsrelation nicht auf Einheiten und Assoziiertheit ankommt.

Lemma 1.11. *In einem kommutativen Ring R gelten folgende Teilbarkeitsbeziehungen.*

(1) -1 *ist eine Einheit, die zu sich selbst invers ist.*
(2) *Jede Einheit teilt jedes Element.*
(3) *Sind a und b assoziiert, so gilt $a|c$ genau dann, wenn $b|c$.*
(4) *Teilt a eine Einheit, so ist a selbst eine Einheit.*

Beweis. Siehe Aufgabe 1.22. □

Für Teilbarkeitsuntersuchungen sind die beiden folgenden Begriffe fundamental. Unter bestimmten Voraussetzungen, etwa wenn ein Hauptidealbereich vorliegt, sind sie äquivalent.

Definition 1.12. Eine Nichteinheit p in einem kommutativen Ring heißt *irreduzibel* (oder *unzerlegbar*), wenn eine Faktorisierung $p = ab$ nur dann möglich ist, wenn einer der Faktoren eine Einheit ist.

Definition 1.13. Eine Nichteinheit $p \neq 0$ in einem kommutativen Ring R heißt *prim* (oder ein *Primelement*), wenn folgendes gilt: Teilt p ein Produkt ab mit $a, b \in R$, so teilt es einen der Faktoren.

Eine Einheit ist also nach Definition nie ein Primelement. Dies ist eine Verallgemeinerung des Standpunktes, dass 1 keine Primzahl ist. Dabei ist die 1 nicht deshalb keine Primzahl, weil sie „zu schlecht“ ist, sondern weil sie „zu gut“ ist.

Integritätsbereiche

Vor dem nächsten Lemma erinnern wir an den Begriff des Integritätsbereiches. Häufig wird die Teilbarkeitstheorie nur für Integritätsbereiche entwickelt.

Definition 1.14. Ein kommutativer, nullteilerfreier, von null verschiedener Ring heißt *Integritätsbereich*.

Ein *Nullteiler* ist ein Element x mit der Eigenschaft, dass es ein von 0 verschiedenes Element y mit $xy = 0$ gibt. Die Null ist in einem vom Nullring verschieden Ring stets ein Nullteiler. *Nullteilerfrei* bedeutet, dass die 0 der einzige Nullteiler ist bzw. dass alle von 0 verschiedenen Elemente keine Nullteiler oder *Nichtnullteiler* sind. Nullteilerfrei kann man auch so formulieren, dass aus einer Gleichung $xy = 0$ folgt, dass $x = 0$ oder $y = 0$ ist.

DEFINITION 1.15. Ein kommutativer Ring R heißt *Körper*, wenn $R \neq 0$ ist und wenn jedes von 0 verschiedene Element ein multiplikatives Inverses besitzt.

In einem Körper sind also alle von 0 verschiedenen Elemente Einheiten (und insbesondere Nichtnullteiler). Körper sind also insbesondere Integritätsbereiche. In einem Körper ist die Teilbarkeitsbeziehung uninteressant, da jedes von 0 verschiedene Element jedes andere Element teilt.

LEMMA 1.16. *In einem Integritätsbereich ist ein Primelement stets irreduzibel.*

Beweis. Angenommen, wir haben eine Zerlegung $p = ab$. Wegen der Primeigenschaft teilt p einen Faktor, sagen wir $a = ps$. Dann ist $p = psb$ bzw. $p(1 - sb) = 0$. Da p kein Nullteiler ist, folgt $1 = sb$, so dass also b eine Einheit ist. □