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

Zahlentheorie

Vorlesung 2

Ideale

Alle Vielfachen der 5, also $\mathbb{Z}5$, bilden ein Ideal im Sinne der folgenden Definition.

DEFINITION 2.1. Eine nichtleere Teilmenge $\mathfrak{a}$ eines kommutativen Ringes R heißt *Ideal*, wenn die beiden folgenden Bedingungen erfüllt sind:

(1) Für alle $a, b \in \mathfrak{a}$ ist auch $a + b \in \mathfrak{a}$.
(2) Für alle $a \in \mathfrak{a}$ und $r \in R$ ist auch $ra \in \mathfrak{a}$.

DEFINITION 2.2. Zu einer Familie von Elementen $a_j \in R$, $j \in J$, in einem kommutativen Ring R bezeichnet $(a_j : j \in J)$ das von den a_j *erzeugte Ideal*. Es besteht aus allen (endlichen) *Linearkombinationen*

$$\sum_{j \in J_0} r_j a_j \, ,$$

wobei $J_0 \subseteq J$ eine endliche Teilmenge und $r_j \in R$ ist.

DEFINITION 2.3. Ein Ideal $\mathfrak{a}$ in einem kommutativen Ring R der Form

$$\mathfrak{a} = (a) = Ra = \{ra : r \in R\}.$$

heißt *Hauptideal*.

Mit dem Idealbegriff lassen sich Teilbarkeitsbeziehungen ausdrücken.

LEMMA 2.4. *Sei R ein kommutativer Ring und $a, b \in R$. Dann gelten folgende Aussagen.*

(1) *Das Element a ist ein Teiler von b (also $a|b$), genau dann, wenn $(b) \subseteq (a)$.*
(2) *a ist eine Einheit genau dann, wenn $(a) = R = (1)$.*
(3) *Ist R ein Integritätsbereich, so gilt $(a) = (b)$ genau dann, wenn a und b assoziiert sind.*

Beweis. Siehe Aufgabe 2.20. □

DEFINITION 2.5. Ein kommutativer Ring, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealring*. Ein integrer Hauptidealring heißt *Hauptidealbereich*.

Größter gemeinsamer Teiler

DEFINITION 2.6. Sei R ein kommutativer Ring und $a_1, \ldots, a_k \in R$. Dann heißt ein Element $t \in R$ *gemeinsamer Teiler* der $a_1, \ldots, a_k$, wenn t jedes a_i teilt ($i = 1, \ldots, k$). Ein Element $g \in R$ heißt *größter gemeinsamer Teiler* der $a_1, \ldots, a_k$, wenn g ein gemeinsamer Teiler ist und wenn jeder gemeinsame Teiler t dieses g teilt.

Die Elemente $a_1, \ldots, a_k$ heißen *teilerfremd*, wenn 1 ihr größter gemeinsamer Teiler ist.

BEMERKUNG 2.7. Eine Einheit ist immer ein gemeinsamer Teiler für jede Auswahl von Elementen. Ein größter gemeinsamer Teiler muss im Allgemeinen nicht existieren. Ist t ein gemeinsamer Teiler der $a_1, \ldots, a_k$ und u eine Einheit, so ist auch ut ein gemeinsamer Teiler der $a_1, \ldots, a_k$. Die Elemente $a_1, \ldots, a_k$ sind *teilerfremd* genau dann, wenn jeder gemeinsame Teiler davon eine Einheit ist (es gibt noch andere Definitionen von teilerfremd, die nicht immer inhaltlich mit dieser übereinstimmen).

LEMMA 2.8. *Sei R ein kommutativer Ring, $a_1, \ldots, a_k \in R$ und $\mathfrak{a} = (a_1, \ldots, a_k)$ das davon erzeugte Ideal. Ein Element $t \in R$ ist ein gemeinsamer Teiler von $a_1, \ldots, a_k \in R$ genau dann, wenn $\mathfrak{a} \subseteq (t)$ ist, und t ist ein größter gemeinsamer Teiler genau dann, wenn für jedes $s \in R$ mit $\mathfrak{a} \subseteq (s)$ folgt, dass $(t) \subseteq (s)$ ist. Ein größter gemeinsamer Teiler erzeugt also ein minimales Hauptoberideal von $\mathfrak{a}$.*

Beweis. Aus $\mathfrak{a} = (a_1, \ldots, a_k) \subseteq (t)$ folgt sofort $(a_i) \subseteq (t)$ für $i = 1, \ldots, k$, was gerade bedeutet, dass t diese Elemente teilt, also ein gemeinsamer Teiler ist. Sei umgekehrt t ein gemeinsamer Teiler. Dann ist $a_i \in (t)$ und da $\mathfrak{a} = (a_1, \ldots, a_k)$ das kleinste Ideal ist, das alle a_i enthält, muss $\mathfrak{a} \subseteq (t)$ gelten. Der zweite Teil folgt sofort aus dem ersten. □

Bevor wir mit der Teilbarkeitstheorie für Hauptidealbereiche fortfahren, wollen wir zunächst zeigen, dass die ganzen Zahlen einen Hauptidealbereich bilden. Dies geschieht über den Begriff des Euklidischen Bereiches, der an die Division mit Rest anknüpft. Im Ring der ganzen Zahlen gilt die Division mit Rest, ebenso in einem Polynomring in einer Variablen über einem Körper. Ihre Bedeutung liegt grob gesprochen darin, dass sie ein Maß dafür liefert, wie weit eine Zahl davon entfernt ist, eine andere zu teilen.

Division mit Rest

Für ganze Zahlen a, b, $b \neq 0$, gibt es (eindeutig bestimmte) ganze Zahlen q, r mit

$$a = qb + r \text{ und } 0 \leq r < |b| \ .$$

Dabei bezeichnet $|\ |$ den Betrag einer ganzen Zahl. Das Symbol q soll dabei an Quotient erinnern und r an Rest. Teilt man die Gleichung durch b, so erhält man in $\mathbb{Q}$ die Beziehung

$$\frac{a}{b} = q + \frac{r}{b} \text{ mit } q \in \mathbb{Z} \text{ und } 0 \leq \frac{r}{b} < 1\,.$$

DEFINITION 2.9. Ein *euklidischer Bereich* (oder *euklidischer Ring*) ist ein Integritätsbereich R, für den eine Abbildung $\delta : R \setminus \{0\} \to \mathbb{N}$ existiert, die die folgende Eigenschaft erfüllt:

Für Elemente a, b mit $b \neq 0$ gibt es $q, r \in R$ mit

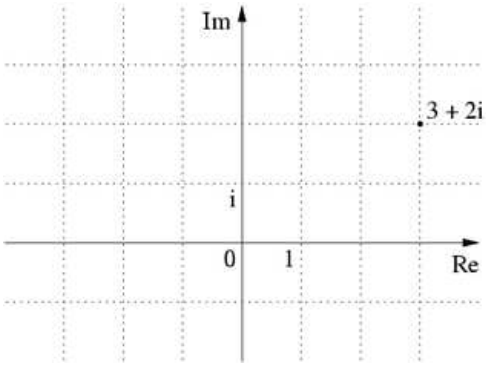
$$a = qb + r \text{ und } r = 0 \text{ oder } \delta(r) < \delta(b)\,.$$

Die in der Definition auftauchende Abbildung δ nennt man auch *euklidische Funktion*. Die ganzen Zahlen $\mathbb{Z}$ bilden also einen euklidischen Ring mit dem Betrag als euklidischer Funktion.

BEISPIEL 2.10. Für einen Körper K ist der Polynomring $K[X]$ in einer Variablen ein euklidischer Bereich, wobei die euklidische Funktion δ durch die Gradfunktion gegeben ist. Viele Parallelen zwischen dem Polynomring $K[X]$ und $\mathbb{Z}$ beruhen auf dieser Eigenschaft. Die Gradfunktion hat die Eigenschaft

$$\delta(fg) \;=\; \delta(f) + \delta(g).$$

BEISPIEL 2.11. Eine Gaußsche Zahl z ist durch $z = a + b\mathrm{i}$ gegeben, wobei a und b ganze Zahlen sind. Die Menge dieser Zahlen wird mit $\mathbb{Z}[\mathrm{i}]$ bezeichnet. Die Gaußschen Zahlen sind die Gitterpunkte, d.h. die Punkte mit ganzzahligen Koordinaten, in der komplexen Ebene. Sie bilden mit komponentenweiser Addition und mit der induzierten komplexen Multiplikation einen kommutativen Ring.



Gaußsche Zahlen als Gitterpunkte in der komplexen Zahlenebene

Eine euklidische Funktion ist durch die Norm N gegeben, die durch $N(a + b\mathrm{i}) := a^2 + b^2$ definiert ist. Man kann auch $N(z) \;=\; z \cdot \bar{z}$ schreiben, wobei $\bar{z}$ die komplexe Konjugation bezeichnet. Die Norm ist das Quadrat des komplexen Absolutbetrages und wie dieser multiplikativ, also $N(zw) = N(z)N(w)$.

Mit der Norm lassen sich auch leicht die Einheiten von $\mathbb{Z}$[i] bestimmen: ist $wz = 1$, so ist auch $N(zw) = N(z)N(w) = 1$, also $N(z) = 1$. Damit sind genau die Elemente $\{1, -1, \mathrm{i}, -\mathrm{i}\}$ diejenigen Gaußschen Zahlen, die Einheiten sind.

LEMMA 2.12. *Der Ring der Gaußschen Zahlen ist mit der Normfunktion ein euklidischer Bereich.*

Beweis. Seien $w, z \in \mathbb{Z}[i]$, $z \neq 0$. Wir betrachten den Quotienten

$$\frac{w}{z} = \frac{w\bar{z}}{z\bar{z}} = q_1 + q_2 i.$$

Dies ist eine komplexe Zahl mit rationalen Koeffizienten, also $q_1, q_2 \in \mathbb{Q}$. Es gibt ganze Zahlen a_1, a_2 mit $|q_1 - a_1|, |q_2 - a_2| \leq 1/2$. Damit ist

$$q_1 + q_2 i = a_1 + a_2 i + (q_1 - a_1) + (q_2 - a_2)i$$

mit $a_1 + a_2 i \in \mathbb{Z}[i]$. Ferner ist

$$\begin{aligned} N((q_1 - a_1) + (q_2 - a_2)i) &= (q_1 - a_1)^2 + (q_2 - a_2)^2 \\ &\leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 \\ &< 1. \end{aligned}$$

Multiplikation mit z ergibt

$$w = z(a_1 + a_2 i) + z((q_1 - a_1) + (q_2 - a_2)i)$$

und aus der Multiplikativität der Norm folgt

$$N\left(z\left((q_1 - a_1) + (q_2 - a_2)i\right)\right) = N(z)N\left((q_1 - a_1) + (q_2 - a_2)i\right) < N(z).$$

□

Für eine unvollständige Liste von Primfaktorzerlegungen im Ring der Gaußschen Zahlen siehe hier oder hier.

Folgendes Lemma hilft bei der Bestimmung der Primelemente der Gaußschen Zahlen und in ähnlichen Ringen.

LEMMA 2.13. *Sei R ein euklidischer Bereich mit einer multiplikativen euklidischen Funktion*

$$N\colon\ R \setminus \{0\} \longrightarrow \mathbb{N}_+$$

(es werden also nur positive Werte angenommen). Ist dann für $f \in R$ die Zahl $N(f)$ prim, so ist f irreduzibel in R.

Beweis. Sei $f = gh$ eine Faktorzerlegung. Dann ist $N(f) = N(g)N(h)$ und da nach Voraussetzung $N(f)$ eine Primzahl ist, folgt, dass einer der Faktoren, sagen wir $N(h)$, eine Einheit ist, also $N(h) = 1$. Wir wenden auf 1 und h die Division mit Rest an und erhalten

$$1 = qh + r,$$

wobei $r = 0$ ist oder $N(r) < N(h) = 1$. Letzteres ist aber ausgeschlossen, so dass $r = 0$ sein muss und damit ist h eine Einheit. Also ist f irreduzibel. □

Wir werden später sehen, dass in euklidischen Bereichen irreduzible Elemente bereits prim sind. Das vorstehende Lemma ist also ein Kriterium für Primelemente. Die Umkehrung gilt übrigens nicht. Z. B. ist 3 ein Primelement in $\mathbb{Z}[i]$, aber $N(3) = 9$ ist keine Primzahl.

Nach den Gaußschen Zahlen sind die sogenannten Eisenstein-Zahlen ein wichtiges Beispiel für quadratische Zahlbereiche.

Beispiel 2.14. Die Eisenstein-Zahlen sind komplexe Zahlen der Form

$$z = a + b\left(\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3}\right)$$

mit ganzen Zahlen a und b. Insbesondere ist

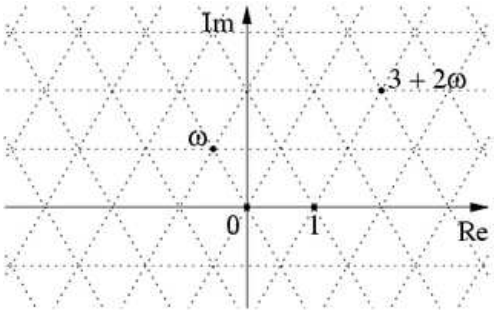
$$\omega = -\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3} = e^{2\pi \mathrm{i}/3}$$

eine Eisenstein-Zahl. Diese Zahl ist zugleich eine (primitive) dritte Einheitswurzel (also $\omega^3 = 1$), so dass der Ring der Eisenstein-Zahlen zugleich der dritte Kreisteilungsring ist. Wegen $\omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1)$ und

$$\omega \neq 1$$

gilt die Gleichung

$$\omega^2 + \omega + 1 = 0.$$



Eisenstein-Zahlen als Punkte eines Dreiecksgitters in der komplexen Zahlenebene

Die Eisenstein-Zahlen enthalten den Ring $\mathbb{Z}[\sqrt{-3}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-3}$. Im obigen Bild besteht dieser Ring aus jeder zweiten horizontalen Zeile des Gitters und ist damit ein rechtwinkliges Gitter. Es gilt der folgende Satz.

Satz 2.15. *Für den Ring $\mathbb{Z}[\sqrt{-3}]$ ist die Norm (das Quadrat des komplexen Betrages) keine euklidische Funktion, aber für den Ring der Eisenstein-Zahlen $\mathbb{Z}[\omega]$ mit $\omega = \frac{-1+\sqrt{3}i}{2}$ ist die Norm eine euklidische Funktion.*

Beweis. Wie dem Beweis zur Euklidizität der Gaußschen Zahlen zu entnehmen ist, ist für einen Unterring der komplexen Zahlen der Form $\Gamma = \mathbb{Z} \oplus \mathbb{Z}x$ (mit $x \notin \mathbb{R}$) die Norm eine euklidische Funktion genau dann, wenn sich zu jedem Element $z \in \mathbb{Q}(\Gamma) = \mathbb{Q} \oplus \mathbb{Q}x$ ein Element $u \in \Gamma$ findet, das zu z einen Abstand kleiner als 1 besitzt. Sei zunächst $\Gamma = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-3}$. Das Element $\omega = \frac{-1+\sqrt{-3}}{2} \in \mathbb{Q}(\Gamma)$ hat den minimalen Abstand zu den vier Gitterpunkten $(0,0), (-1,0), (0,\sqrt{3}), (-1,\sqrt{3})$, und dieser ist stets

$$\left|\frac{-1+\sqrt{-3}}{2}\right| = \sqrt{\frac{1}{4}+\frac{3}{4}} = 1.$$

Für den Ring der Eisenstein-Zahlen $\mathbb{Z}[\omega]$ sind die Gittermaschen gleichmäßige Dreiecke mit Seitenlänge eins, und jede komplexe Zahl hat zu mindestens einem Gitterpunkt einen Abstand < 1. □

Es lässt sich zeigen, dass der Ring $\mathbb{Z}[\sqrt{-3}]$ auch keine andere euklidische Funktion besitzt (er ist auch kein Hauptidealbereich, noch nicht mal, wie wir später sehen und erklären werden, normal).

Eine wichtige Konsequenz aus der Existenz einer euklidischen Funktion ist, dass ein Hauptidealbereich vorliegt.

Satz 2.16. *Ein euklidischer Bereich ist ein Hauptidealbereich.*

Beweis. Sei I ein von 0 verschiedenes Ideal. Betrachte die nichtleere Menge

$$\{\delta(a) | \, a \in I, \, a \neq 0\} \, .$$

Diese Menge hat ein Minimum m, das von einem Element $b \in I, \, b \neq 0$ herrührt, sagen wir $m = \delta(b)$. Wir behaupten, dass $I = (b)$ ist. Dabei ist die Inklusion „$\supseteq$“ klar. Zum Beweis der Inklusion „$\subseteq$“ sei $a \in I$ gegeben. Aufgrund der Definition eines euklidischen Bereiches gilt $a = qb + r$ mit $r = 0$ oder $\delta(r) < \delta(b)$. Wegen $r \in I$ und der Minimalität von $\delta(b)$ kann der zweite Fall nicht eintreten. Also ist $r = 0$ und a ist ein Vielfaches von b. □

Abbildungsverzeichnis