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

Zahlentheorie

Vorlesung 25

Die Divisorenklassengruppe

DEFINITION 25.1. Sei R ein Zahlbereich. Es sei $\mathrm{Div}(R)$ die Gruppe der Divisoren und $H \subseteq \mathrm{Div}(R)$ sei die Untergruppe der Hauptdivisoren Dann nennt man die Restklassengruppe

$$\mathrm{KG}(R) = \mathrm{Div}(R)/H$$

die *Divisorenklassengruppe* von R.

Die Divisorenklassengruppe wird häufig auch als *Idealklassengruppe* oder einfach als *Klassengruppe* bezeichnet. Sie ist kommutativ. Ihre Elemente sind Äquivalenzklassen und werden durch Divisoren repräsentiert, wobei zwei Divisoren genau dann die gleiche Klasse repräsentieren, wenn ihre Differenz ein Hauptdivisor ist. Sie heißen *Divisorklassen* oder *Idealklassen*. Ein späteres Hauptresultat - das wir aber nur für quadratische Zahlbereiche beweisen werden - wird sein, dass die Klassengruppe endlich ist. Sie ist eine wesentliche (ko)-homologische Invariante eines Zahlbereichs und enthält wesentliche Informationen über diesen. Generell lässt sich sagen, dass ihre Größe zum Ausdruck bringt, wie weit ein Zahlbereich von der Faktorialität entfernt ist. Der nächste Satz charakterisiert die Faktorialität dadurch, dass die Klassengruppe trivial ist.

SATZ 25.2. *Sei R ein Zahlbereich und es bezeichne $\mathrm{KG}(R)$ die Divisorenklassengruppe von R. Dann sind folgende Aussagen äquivalent.*

(1) *R ist ein Hauptidealbereich.*
(2) *R ist faktoriell.*
(3) *Es ist $\mathrm{KG}(R) = 0$.*

Beweis. Die Implikation (1) $\Rightarrow$ (2) folgt aus Satz 3.7.

(2) $\Rightarrow$ (3). Sei also R faktoriell, und sei $\mathfrak{p}$ ein Primideal $\neq 0$. Sei $f \in \mathfrak{p}$, $f \neq 0$, mit Primfaktorzerlegung $f = p_1 \cdots p_s$. Da $\mathfrak{p}$ ein Primideal ist, muss einer der Primfaktoren zu $\mathfrak{p}$ gehören, sagen wir $p = p_1 \in \mathfrak{p}$. Dann ist $(p) \subseteq \mathfrak{p}$. Das von p erzeugte Ideal ist ein Primideal, und in einem Zahlbereich ist nach Satz 18.15 jedes von 0 verschiedene Primideal maximal, so dass hier $(p) = \mathfrak{p}$ gelten muss. Auf der Seite der Divisoren gilt aufgrund von Satz 23.12 $\mathrm{div}(p) = 1\mathfrak{p}$,

so dass ein Hauptdivisor vorliegt. Also sind alle Erzeuger der Divisorengruppe Hauptdivisoren und somit ist überhaupt

$$\mathrm{Div}(R) \,=\, H$$

und die Divisorenklassengruppe ist trivial.

(3) $\Rightarrow$ (1). Sei nun $\mathrm{KG}(R) \,=\, 0$ vorausgesetzt. Wir zeigen zunächst, dass jedes Primideal $\mathfrak{p} \neq 0$ ein Hauptideal ist. Nach Voraussetzung ist der Divisor $\mathfrak{p}$ ein Hauptdivisor, so dass $\mathfrak{p} \,=\, \mathrm{div}(p)$ mit einem $p \in R$ gilt. Aufgrund von Satz 23.12 entspricht dies auf der Idealseite der Gleichung $\mathfrak{p} \,=\, (p)$, so dass jedes Primideal ein Hauptideal ist. Für ein beliebiges Ideal $\mathfrak{a} \subseteq R$, $\mathfrak{a} \neq 0$, ist nach Satz 23.14

$$\mathfrak{a} \,=\, \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}.$$

Dies bedeutet aber, mit $\mathfrak{p}_i = (p_i)$, dass $\mathfrak{a}$ ein Hauptideal ist, das von $p_1^{r_1} \cdots p_k^{r_k}$ erzeugt wird. Also liegt ein Hauptidealbereich vor. $\square$

Wir kennen bereits die euklidischen Bereiche $\mathbb{Z}[i]$ und $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, die Hauptidealbereiche sind und deren Klassengruppe somit 0 ist. Der Bereich $\mathbb{Z}[\sqrt{-5}]$ ist hingegen nicht faktoriell und somit kann seine Klassengruppe nicht 0 sein. Wir werden später sehen, dass die Klassengruppe davon einfach $\mathbb{Z}/(2)$ ist, und wir werden allgemein beweisen, dass die Klassengruppe von quadratischen Zahlbereichen immer eine endliche Gruppe ist.

Beispiel 25.3. Wir behaupten, dass im quadratischen Zahlbereich $R = \mathbb{Z}[\sqrt{-5}]$ das Ideal

$$\mathfrak{p} \,=\, (2, 1+\sqrt{-5})$$

kein Hauptideal ist, aber die Eigenschaft besitzt, dass das Quadrat davon ein Hauptideal ist. Insbesondere definiert die zugehörige Idealklasse ein von 0 verschiedenes Element in der Divsorenklassengruppe mit der Eigenschaft, dass das Doppelte davon trivial ist. Es ist

$$\mathfrak{p}^2 \,=\, (4, 2+2\sqrt{-5}, -4+2\sqrt{-5}) \,=\, (2).$$

Dabei ist die Inklusion $\subseteq$ klar und die umgekehrte Inklusion $\supseteq$ ergibt sich aus

$$-4 + (2+2\sqrt{-5}) - (-4+2\sqrt{-5}) \,=\, 2.$$

Wir betrachten nun das Ideal

$$\mathfrak{q} \,=\, (7, 3+\sqrt{-5}).$$

Der Restklassenring ist

$$\mathbb{Z}/(7)[X]/(X^2+5, 3+X) \,\cong\, \mathbb{Z}/(7),$$

so dass ein Primideal mit der Norm 7 vorliegt, das kein Hauptideal ist, da es kein Element mit Norm 7 gibt. Die beiden Ideale $\mathfrak{p}$ und $\mathfrak{q}$ definieren die gleiche Idealklasse. Dazu betrachten wir die Multiplikation

$$Q(R) \longrightarrow Q(R),\, h \longmapsto h\frac{3+\sqrt{-5}}{2}.$$

Wegen

$$2 \cdot \frac{3+\sqrt{-5}}{2} = 3+\sqrt{-5} \in \mathfrak{q}$$

und

$$(1+\sqrt{-5}) \cdot \frac{3+\sqrt{-5}}{2} = \frac{-2+4\sqrt{-5}}{2} = -1+2\sqrt{-5} = -7+2(3+\sqrt{-5}) \in \mathfrak{q}$$

induziert dies einen injektiven R-Modulhomomorphismus

$$\mathfrak{p} \longrightarrow \mathfrak{q},$$

der wegen

$$7 = -(-1+2\sqrt{-5})+2(3+\sqrt{-5})$$

auch surjektiv ist. Somit ist der Quotient der Ideale ein Hauptideal. In Beispiel 27.11 wird darüberhinaus gezeigt, dass die Klassengruppe gleich $\mathbb{Z}/(2)$ ist.

Normeuklidische Bereiche

Wir betrachten nun diejenigen imaginär-quadratischen Zahlbereiche (also $D < 0$), für die die Norm eine euklidische Funktion ist. Wir werden später Beispiele sehen, wo der Ganzheitsring zwar faktoriell, aber nicht euklidisch ist.

Definition 25.4. Sei $D \neq 0, 1$ quadratfrei und A_D der zugehörige quadratische Zahlbereich. Dann heißt A_D *normeuklidisch*, wenn die Normfunktion auf A_D eine euklidische Funktion ist.

Da eine euklidische Funktion nur positive Werte annimmt, kann die Norm allenfalls im imaginär-quadratischen Fall euklidisch sein, da im reell-imaginär quadratischen Fall die Norm auch negative Werte annimmt. Die Euklidizität der Norm bedeutet, dass es zu $a, b \in R$, $b \neq 0$, Elemente z und r mit

$$a = zb + r$$

und $r = 0$ oder

$$N(r) < N(b).$$

Dies kann man auch so sehen, dass es für jede rationales Element $\frac{a}{b} \in Q(R)$ eine ganzzahlige Approximation $z \in R$ mit

$$N\left(\frac{a}{b} - z\right) < 1$$

gibt. Mit Hilfe dieser geometrischen Interpretation charakterisiert der nächste Satz explizit diejenigen imaginär-quadratischen Zahlbereiche, für die A_D normeuklidisch ist.

Satz 25.5. *Sei $D < 0$ quadratfrei und A_D der zugehörige quadratische Zahlbereich. Dann sind folgende Aussagen äquivalent.*

(1) *A_D ist euklidisch.*

(2) A_D *ist normeuklidisch.*
(3) $D = -1, -2, -3, -7, -11$.

Beweis. (1) $\Rightarrow$ (3). Sei A_D euklidisch mit euklidischer Funktion δ. Es sei $z \in A_D$, $z \neq 0$, keine Einheit, so gewählt, dass $\delta(z)$ unter allen Nichteinheiten den minimalen Wert annimmt. Für jedes $w \in A_D$ ist dann

$$w = qz + r \text{ mit } r = 0 \text{ oder } \delta(r) < \delta(z)\,.$$

Wegen der Wahl von z bedeutet dies $r = 0$ oder r ist eine Einheit. Wir betrachten die Restklassenabbildung

$$\varphi\colon\ A_D \longrightarrow A_D/(z).$$

Dabei ist $\varphi(w) = \varphi(r)$. Ab $|D| \geq 4$ gibt es nur die beiden Einheiten 1 und -1, so dass das Bild von φ überhaupt nur aus $0, 1, -1$ besteht. Also ist nach Satz 21.7

$$N(z) = |A_D/(z)| \leq 3$$

Bei $D = 2, 3 \mod 4$ hat nach Satz 20.9 jedes Element aus A_D die Form $z = a + b\sqrt{D}$ $(a, b \in \mathbb{Z})$ mit Norm $N(z) = a^2 + |D|\, b^2$. Damit ist (bei $|D| \geq 4$) $N(z) \leq 3$ nur bei $b = 0$ und $|a| = 1$ möglich, doch dann liegt eine Einheit vor, im Widerspruch zur Wahl von z. In diesem Fall verbleiben also nur die Möglichkeiten $D = -1, -2$.

Bei $D = 1 \mod 4$ hat nach Satz 20.9 jedes Element aus A_D die Form $z = a + b\frac{1+\sqrt{D}}{2}$ $(a, b \in \mathbb{Z})$ mit Norm $N(z) = \left(a + \frac{b}{2}\right)^2 + \frac{|D|b^2}{4}$. Damit ist bei $|D| \geq 12$ die Bedingung $N(z) \leq 3$ wieder nur bei $b = 0$ und $|a| = 1$ möglich, so dass erneut eine Einheit vorliegt. Es verbleiben die Möglichkeiten $D = -3, -7, -11$.

(3) $\Leftrightarrow$ (2). Der Ganzheitsring A_D ist genau dann normeuklidisch, wenn es zu jedem $f \in \mathbb{Q}[\sqrt{D}]$ ein $z \in A_D$ mit $|N(f - z)| < 1$ gibt. Dies bedeutet anschaulich, dass es zu jedem Punkt von $\mathbb{Q}[\sqrt{D}] \subseteq \mathbb{C}$ stets Gitterpunke aus A_D gibt mit einem Abstand kleiner als eins[1] Im Fall $D = 2, 3 \mod 4$ ist $A_D = \mathbb{Z}[\sqrt{D}]$ und es liegt ein rechteckiges Gitter vor, wobei der maximale Abstand im Mittelpunkt eines Gitterrechteckes angenommen wird. Der Abstand zu jedem Eckpunkt ist dort $\sqrt{\frac{1}{4} + \frac{|D|}{4}}$, und dies ist nur für $D = -1, -2$ kleiner als eins.

Im Fall $D = 1 \mod 4$ wird die komplexe Ebene überdeckt von kongruenten gleichschenkligen Dreiecken, mit einer Grundseite der Länge eins und Schenkeln der Länge $\frac{1}{2}\sqrt{1 + |D|}$, deren Eckpunkte jeweils Elemente aus A_D sind. Der Punkt innerhalb eines solchen Dreiecks mit maximalem Abstand zu den Eckpunkten ist der Mittelpunkt des Umkreises, also der Schnittpunkt

[1] Da $\mathbb{Q}[\sqrt{D}]$ dicht in der komplexen Ebene $\mathbb{C}$ liegt, gilt dies ebenso für alle komplexen Zahlen.

der Mittelsenkrechten. Wir berechnen ihn für das Dreieck mit den Eckpunkten $(0,0),(1,0),\left(\frac{1}{2},\frac{\sqrt{|D|}}{2}\right)$. Die Mittelsenkrechte zur Grundseite ist durch $x=\frac{1}{2}$ gegeben, und die Mittelsenkrechte zum linken Schenkel wird durch $\left(\frac{1}{4},\frac{\sqrt{|D|}}{4}\right)+t\left(\sqrt{|D|},-1\right)$ beschrieben. Gleichsetzen ergibt

$$\frac{1}{4}+t\sqrt{|D|}=\frac{1}{2} \text{ bzw. } t\sqrt{|D|}=\frac{1}{4} \text{ und } t=\frac{1}{4\sqrt{|D|}}\,.$$

Damit ist die zweite Koordinate gleich $\frac{\sqrt{|D|}}{4}-\frac{1}{4\sqrt{|D|}}$ und der gemeinsame Abstand zu den drei Eckpunkten ist die Wurzel aus

$$\frac{1}{4}+\left(\frac{\sqrt{|D|}}{4}-\frac{1}{4\sqrt{|D|}}\right)^2=\frac{1}{4}+\frac{|D|}{16}+\frac{1}{16\,|D|}-\frac{1}{8}=\frac{1}{16}\left(2+|D|+\frac{1}{|D|}\right).$$

Dies (und ebenso die Quadratwurzel) ist kleiner als 1 genau dann, wenn $|D|+\frac{1}{|D|}<14$ ist, was genau bei $D>-13$ der Fall ist und den Möglichkeiten $D=-3,-7,-11$ entspricht.

(2) $\Rightarrow$ (1) ist trivial. □

Bemerkung 25.6. Für ein vorgegebenes quadratfreies D kann man grundsätzlich effektiv entscheiden, ob der quadratische Zahlbereich A_D faktoriell ist oder nicht. Für $D<0$ ist dies genau für

$$D=-1,-2,-3,-7,-11,-19,-43,-67,-163$$

der Fall. Es war bereits von Gauß vermutet worden, dass dies alle sind, es wurde aber erst 1967 von Heegner und Stark bewiesen. Man weiß auch, für welche von diesen D der Ganzheitsbereich euklidisch ist, nämlich nach Satz 25.5 für $D=-1,-2,-3,-7,-11$, aber nicht für die anderen vier Werte.

Für $D>0$ wird vermutet, dass für unendlich viele Werte der Ganzheitsbereich faktoriell ist. Für $D<100$ liegt ein faktorieller Bereich für die Werte

$$D=2,3,5,6,7,11,13,14,17,19,21,23,29,31,33,37,38,41,43,46,47,$$

$$53,57,59,61,62,67,69,71,73,77,83,86,89,93,94,97$$

vor. Dagegen weiß man (Chatland und Davenport 1950), für welche positiven D der Ganzheitsbereich A_D euklidisch ist, nämlich für

$$D=2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73\,.$$