

## Algebraische Zahlentheorie

### Vorlesung 14

#### DIE DIVISORENKLASSENGRUPPE

In vielen Gebieten der Mathematik spielen homologische Methoden eine wichtige Rolle. Dabei wird den mathematischen Objekten eine Gruppe als Invariante zugeordnet, die relevante Information über das ursprüngliche Objekt beinhaltet aber zugleich deutlich einfacher strukturiert ist. Beispiele hierfür sind die Fundamentalgruppe in der Topologie, Homotopie- und Homologiegruppen in der algebraischen Topologie, Kohomologiegruppen zu Garben in der algebraischen Geometrie, ... . Das Verschwinden dieser Gruppen charakterisiert dabei wichtige geometrische Eigenschaften. Die Konstruktion dieser Gruppen ist im Allgemeinen aufwändig und geht dabei häufig über den Weg von „sehr großen“ Gruppen modulo sehr großen Untergruppen (Normalteilern), wobei die Restklassengruppen dann „ziemlich klein“ sind. In diesen Zusammenhang fügt sich auch die Divisorenklassengruppe für algebraische Zahlbereiche ein.

**Definition 14.1.** Es sei  $R$  ein Dedekindbereich. Es sei  $\text{Div}(R)$  die Gruppe der Divisoren und  $H \subseteq \text{Div}(R)$  sei die Untergruppe der Hauptdivisoren. Dann nennt man die Restklassengruppe

$$\text{DKG}(R) = \text{Div}(R)/H$$

die *Divisorenklassengruppe* von  $R$ .

Die Divisorenklassengruppe wird häufig auch als *Idealklassengruppe* oder einfach als *Klassengruppe* bezeichnet. Sie ist kommutativ und wird additiv geschrieben. 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*. Wegen Satz 13.16 kann man die Divisorenklasse auch als die Restklassengruppe zur Gruppe der gebrochenen Ideale modulo der Untergruppe der gebrochenen Hauptideale erhalten. Ein späteres Hauptresultat, das aber einige Vorbereitungen braucht, wird sein, dass die Klassengruppe von Zahlbereichen endlich ist, siehe Satz 26.6. 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 14.2.** *Es sei  $R$  ein Dedekindbereich und es bezeichne  $\text{DKG}(R)$  die Divisorenklassengruppe von  $R$ . Dann sind folgende Aussagen äquivalent.*

- (1)  $R$  ist ein Hauptidealbereich.
- (2)  $R$  ist faktoriell.
- (3) Es ist  $\text{DKG}(R) = 0$ .

*Beweis.* Die Implikation (1)  $\Rightarrow$  (2) folgt aus Satz 2.19.

(2)  $\Rightarrow$  (3). Es 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 Dedekindbereich ist nach Definition jedes von 0 verschiedene Primideal maximal, sodass hier  $(p) = \mathfrak{p}$  gelten muss. Auf der Seite der Divisoren gilt aufgrund von Satz 11.13  $\text{div}(p) = 1\mathfrak{p}$ , sodass ein Hauptdivisor vorliegt. Also sind alle Erzeuger der Divisorengruppe Hauptdivisoren und somit ist überhaupt

$$\text{Div}(R) = H$$

und die Divisorenklassengruppe ist trivial.

(3)  $\Rightarrow$  (1). Es sei nun  $\text{DKG}(R) = 0$  vorausgesetzt. Wir zeigen zunächst, dass jedes Primideal  $\mathfrak{p} \neq 0$  ein Hauptideal ist. Nach Voraussetzung ist der Divisor  $\mathfrak{p}$  ein Hauptdivisor, sodass  $\mathfrak{p} = \text{div}(p)$  mit einem  $p \in R$  gilt. Aufgrund von Satz 11.13 entspricht dies auf der Idealseite der Gleichung  $\mathfrak{p} = (p)$ , sodass jedes Primideal ein Hauptideal ist. Für ein beliebiges Ideal  $\mathfrak{a} \subseteq R$ ,  $\mathfrak{a} \neq 0$ , ist nach Satz 12.2

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

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.  $\square$

Insofern ist die erste wichtige Frage bei einem Dedekindbereich, ob seine Klassengruppe gleich 0 ist oder nicht.

**Beispiel 14.3.** Wir behaupten, dass im quadratischen Zahlbereich  $R = \mathbb{Z}[\sqrt{-5}]$  das Ideal

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

kein Hauptideal ist, was in Beispiel 10.7 gezeigt wurde, aber die Eigenschaft besitzt, dass das Quadrat davon ein Hauptideal ist. Insbesondere definiert die zugehörige Idealklasse ein von 0 verschiedenes Element in der Divisorenklassengruppe 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

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

sodass 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

$$\mathfrak{p} \cdot \left( \frac{3 + \sqrt{-5}}{2} \right) = \mathfrak{q}$$

als gebrochene Ideale. In Beispiel 26.12 wird darüber hinaus gezeigt, dass die Klassengruppe von  $R$  gleich  $\mathbb{Z}/(2)$  ist.

#### DIE DIVISORENKLASSENGRUPPE UNTER HOMOMORPHISMEN

Ein wichtiger Aspekt von homologischen Invarianten ist, dass sie nicht nur den Objekten Gruppen zuordnen, sondern auch den richtigen Abbildungen zwischen den Objekten Gruppenhomomorphismen. Wir besprechen zuerst den Fall einer Nenneraufnahme  $R \rightarrow R_S$  zu einem multiplikativen System  $S \subseteq R$  in einem Dedekindbereich. Nach Proposition 5.4 (2) entsprechen die Primideale von  $R_S$  den Primidealen von  $R$ , die mit  $S$  einen leeren Schnitt haben. Bei gegebenem  $S$  kann man also die Primideale von  $R$  dahingehend aufteilen, ob sie einen leeren oder einen nichtleeren Durchschnitt mit  $S$  haben.

**Lemma 14.4.** *Es sei  $R$  ein Dedekindbereich und es sei  $S \subseteq R$ ,  $0 \notin S$ , ein multiplikatives System mit der Nenneraufnahme  $R_S$ . Dann liegt eine exakter Komplex*

$$1 \longrightarrow R^\times \longrightarrow R_S^\times \longrightarrow \mathbb{Z}^{\{\mathfrak{p} \mid \mathfrak{p} \cap S \neq \emptyset\}} \longrightarrow \text{DKG}(R) \longrightarrow \text{DKG}(R_S) \longrightarrow 0$$

vor. Dabei ordnet die dritte Abbildung einer Einheit  $f \in R_S^\times$  die Einschränkung des Hauptdivisors auf die angegebene Primidealmenge zu. Die vierte Abbildung ordnet einen Divisor  $\sum_{\mathfrak{p} \cap S \neq \emptyset} n_{\mathfrak{p}} \mathfrak{p}$  auf die zugehörige Klasse in  $\text{DKG}(R)$  zu.

*Beweis.* Die Injektivität links ist klar. Die Einheiten aus  $R$  haben überhaupt an jedem Primideal die Ordnung 0, deshalb ist an der nächsten Stelle die Zusammensetzung die triviale Abbildung. Sei  $f \in R_S^\times$  derart, dass es unter der folgenden Abbildung auf 0 geht. Das bedeutet, dass es an allen Primidealen, die nicht zu  $R_S$  gehören, die Ordnung 0 besitzt. Da es eine Einheit in  $R_S$  ist, hat es auch an allen Primidealen, die zu  $R_S$  gehören, und damit überhaupt an jedem Primideal von  $R$  die Ordnung 0 und ist somit eine Einheit in  $R$ .

Die dritte Abbildung ist einfach die Hauptdivisorabbildung, da in den Primidealen, die zu  $S$  disjunkt sind, die Ordnung einer Einheit aus  $R_S$  stets 0 ist und sich der relevante Teil des Hauptdivisors in den angegebenen Primidealen abspielt. Die zusammengesetzte Abbildung ist daher die Nullabbildung, da in der Klassengruppe die Hauptdivisoren zu 0 gemacht werden. Wenn ein Divisor  $\sum_{\mathfrak{p} \cap S \neq \emptyset} n_{\mathfrak{p}} \mathfrak{p}$  in der Klassengruppe von  $R$  zu 0 wird, so bedeutet dies die Existenz eines  $f \in Q(R) \setminus \{0\}$  mit

$$\text{div}(f) = \sum_{\mathfrak{p} \cap S \neq \emptyset} n_{\mathfrak{p}} \mathfrak{p}.$$

Dabei sind dann insbesondere die Ordnungen von  $f$  an den Primidealen, die mit  $S$  einen leeren Durchschnitt haben, gleich 0, und dann gehört  $f$  zu  $R_S$  und ist dort eine Einheit.

Ein Divisor mit der angegebenen Trägermenge wird in der Klassengruppe von  $R_S$  zu 0, da diese Primideale in der Nenneraufnahme nicht überleben. Es sei  $[D] \in \text{DKG}(R)$  eine Divisoroklasse, repräsentiert durch  $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p}$ , die in der Divisorenklassengruppe von  $R_S$  zu 0 wird. Wir schreiben  $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p} = \sum_{\mathfrak{p} \cap S \neq \emptyset} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\mathfrak{p} \cap S = \emptyset} n_{\mathfrak{p}} \mathfrak{p} = D_1 + D_2$ . Unter der Abbildung wird dies nach  $[D_2]$  abgebildet. Aus

$$D_2 = \text{div}(f)$$

in der Divisorengruppe zu  $R_S$  folgt, dass die Differenz zwischen  $D$  und  $\text{div}(f)$  in der Divisorengruppe zu  $R$  mit Primidealen geschrieben werden kann, die zu  $S$  einen nichtleeren Durchschnitt haben. Diese Differenz kommt also von rechts. Die Surjektivität an der letzten Stelle ist klar.  $\square$

Die Abbildung  $\text{DKG}(R) \rightarrow \text{DKG}(R_S)$  fügt sich in das kommutative Diagramm

$$\begin{array}{ccc} \text{Div}(R) & \longrightarrow & \text{Div}(R_S) \\ \downarrow & & \downarrow \\ \text{DKG}(R) & \longrightarrow & \text{DKG}(R_S) \end{array}$$

ein, wobei die obere horizontale Abbildung einen Divisor  $\sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p}$  von  $R$  einfach auf denjenigen Divisor von  $R_S$  abbildet, bei dem die Primideale  $\mathfrak{p}$  mit  $\mathfrak{p} \cap S \neq \emptyset$  ignoriert („vergessen“) werden. Dies entspricht der Abbildung, bei der ein gebrochenes Ideal  $\mathfrak{f}$  auf das Erweiterungsideal  $\mathfrak{f}R_S$  abgebildet wird.

**Lemma 14.5.** *Zu einer Erweiterung von Dedekindbereichen  $R \subseteq S$  gehört in funktorieller Weise ein Gruppenhomomorphismus*

$$\mathrm{DKG}(R) \longrightarrow \mathrm{DKG}(S), [\mathfrak{a}] \longmapsto [\mathfrak{a}S].$$

*Beweis.* Wir gehen von der Zuordnung aus, die jedem von 0 verschiedenen Ideal  $\mathfrak{a}$  von  $R$  das Erweiterungsideal  $\mathfrak{a}S$  zuordnet, das ebenfalls von 0 verschieden ist. Diese Zuordnung ist mit dem Produkt von Idealen verträglich. Deshalb liegt ein Monoidhomomorphismus vor. Ein gebrochenes Ideal kann man nach Aufgabe 13.31 in der Form  $\mathfrak{a}\mathfrak{b}^{-1}$  mit Idealen  $\mathfrak{a}, \mathfrak{b}$  schreiben und diesem das gebrochene Ideal  $\mathfrak{a}S(\mathfrak{b}S)^{-1}$  zuordnen. Dies ist wohldefiniert und so erhält man einen Gruppenhomomorphismus von der Gruppe der gebrochenen Ideale  $\neq 0$  von  $R$  in die Gruppe der gebrochenen Ideale  $\neq 0$  von  $S$ . Das Erweiterungsideal eines Hauptideals ist wieder ein Hauptideal, und deshalb werden gebrochene Hauptideale auf gebrochene Hauptideale abgebildet. Der Satz vom induzierten Homomorphismus ergibt somit einen Gruppenhomomorphismus

$$\mathrm{DKG}(R) \longrightarrow \mathrm{DKG}(S).$$

□

Insgesamt liegt das kommutative Diagramm

$$\begin{array}{ccccc} \text{Gebrochene Hauptideale}(R) & \longrightarrow & \text{Gebrochene Ideale}(R) & \longrightarrow & \mathrm{DKG}(R) \\ \downarrow & & \downarrow & & \downarrow \\ \text{Gebrochene Hauptideale}(S) & \longrightarrow & \text{Gebrochene Ideale}(S) & \longrightarrow & \mathrm{DKG}(S) \end{array}$$

vor. Auf der Divisorebene wird dabei einem Primdivisor  $\mathfrak{p}$  der Divisor zum Ideal  $\mathfrak{p}S$  zugeordnet. Das Erweiterungsideal zu  $\mathfrak{p}$  beschreibt dabei die Faser der Spektrumsabbildung  $\mathrm{Spek}(S) \rightarrow \mathrm{Spek}(R)$  über  $\mathfrak{p}$ . Dies ist insbesondere bei endlichen Erweiterungen von Dedekindbereichen relevant. Man kann sich fragen, ob die Abbildung zwischen den Klassengruppen stets injektiv ist, oder ob umgekehrt ein nichttriviales Ideal zu einem Hauptideal werden kann. Dies ist in der Tat der Fall.

**Beispiel 14.6.** Wir betrachten im quadratischen Zahlbereich  $R$  zu  $D = -5$  das Ideal  $\mathfrak{p} = (2, 1 + \sqrt{-5})$ , das nach Beispiel 10.7 kein Hauptideal ist. Es sei  $S$  der ganze Abschluss von  $R$  (oder von  $\mathbb{Z}$ ) im Erweiterungskörper  $L = \mathbb{Q}[\sqrt{-5}, \sqrt{2}]$  vom Grad vier über  $\mathbb{Q}$ . Wir haben also eine Kette

$$\mathbb{Z} \subset R \subset S$$

von Zahlbereichen. Wir behaupten, dass das Erweiterungsideal

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

ein Hauptideal in  $S$  ist, und zwar behaupten wir, dass  $\sqrt{2}$  ein Idealerzeuger davon ist. Dazu betrachten wir zunächst das rationale Element  $z = \frac{\sqrt{2} + \sqrt{2} \cdot \sqrt{-5}}{2} = \frac{1 + \sqrt{-5}}{\sqrt{2}} \in L$ . Wegen

$$z^2 = \left( \frac{\sqrt{2} + \sqrt{2} \cdot \sqrt{-5}}{2} \right)^2 = \frac{2 - 2 \cdot 5 + 4\sqrt{-5}}{4} = -2 + \sqrt{-5} \in R$$

erfüllt  $z$  eine Ganzheitsgleichung über  $R$  und gehört somit zu  $S$  (ebenso, wenn im Zähler ein Minuszeichen steht). Die Gleichheit

$$\mathfrak{p}S = (\sqrt{2})$$

folgt einerseits aus

$$2 = \sqrt{2} \cdot \sqrt{2}$$

und

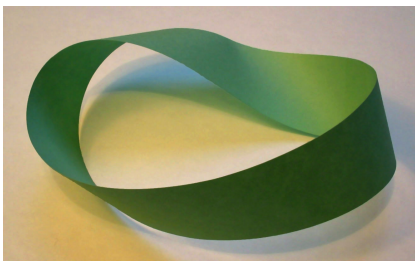
$$1 + \sqrt{-5} = z \cdot \sqrt{2}$$

und andererseits aus

$$\begin{aligned} -\sqrt{2} \cdot 2 + \frac{1 - \sqrt{-5}}{\sqrt{2}}(1 + \sqrt{-5}) &= -\sqrt{2} \cdot 2 + \frac{6}{\sqrt{2}} \\ &= -\sqrt{2} \cdot 2 + 3 \cdot \sqrt{2} \\ &= \sqrt{2}(-2 + 3) \\ &= \sqrt{2}. \end{aligned}$$

Es gilt sogar, dass man im zahlentheoretischen Kontext jede Klasse trivialisieren kann. Dies bedeutet aber nicht, dass es zu jedem Zahlbereich eine faktorielle Erweiterung gibt, da durch die Trivialisierung typischerweise „an anderer Stelle“ nichttriviale Klassen auftreten.

**Beispiel 14.7.** Wir betrachten den kommutativen Ring  $R = \mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$ , der dem Einheitskreis in dem Sinne entspricht, dass die Primideale der Form  $(X - a, Y - b)$  darin den reellen Punkten des Kreis entsprechen. Dies ist ein Dedekindbereich, wobei die Normalität aus der Glattheit des Kreises folgt.



Das Möbiusband.

Das Ideal  $\mathfrak{p} = (X, Y - 1)$  ist ein Primideal darin, das kein Hauptideal ist. Für das Produkt dieses Ideals mit sich selbst haben wir

$$(X, Y - 1)^2 = (X^2, XY - X, (Y - 1)^2) = (Y - 1),$$

wobei die Inklusion  $\subseteq$  klar ist und sich die andere Inklusion aus

$$\frac{1}{2}(-X^2 - (Y - 1)^2) = \frac{1}{2}(-1 + Y^2 - (Y - 1)^2) = Y - 1$$

ergibt. Da  $Y - 1$  in  $R$  keine Quadratwurzel (und auch nicht multipliziert mit einer Einheit) besitzt, ist  $\mathfrak{p}$  kein Hauptideal. Dieses Ideal ist eine algebraische Realisierung des Möbiusbandes (ein Ideal definiert eine invertierbare Garbe und ein Geradenbündel; das Möbiusband ist das nichttriviale Geradenbündel auf dem Einheitskreis).

Wir betrachten den Ringhomomorphismus

$$R = \mathbb{R}[X, Y]/(X^2 + Y^2 - 1) \longrightarrow S = \mathbb{R}[U, V]/(U^2 + V^2 - 1),$$

$$(X, Y) \longmapsto (U^2 - V^2, 2UV),$$

des Ringes in sich (wir schreiben rechts  $S$ , um die unterschiedlichen Rollen zu betonen). Wegen

$$\begin{aligned} X^2 + Y^2 &= (U^2 - V^2)^2 + (2UV)^2 \\ &= U^4 - 2U^2V^2 + V^4 + 4U^2V^2 \\ &= U^4 + 2U^2V^2 + V^4 \\ &= (U^2 + V^2)^2 \\ &= 1 \end{aligned}$$

ist dies wohldefiniert (es handelt sich um die komplexe Quadrierung eingeschränkt auf den Einheitskreis). Es handelt sich um eine ganze Ringerweiterung. Das Erweiterungsideal zu  $(X, Y - 1)$  ist

$$(U^2 - V^2, 2UV - 1) = (1 - 2V^2, 2UV - 1) = (U - V),$$

also ein Hauptideal. Dies beruht auf

$$\begin{aligned} U^2 - V^2 &= (U + V)(U - V), \\ 2UV - 1 &= 2UV - U^2 - V^2 = (V - U)(U - V) \end{aligned}$$

und

$$U - V = V(U^2 - V^2) - U(2UV - 1).$$



## ABBILDUNGSVERZEICHNIS

- Quelle = Möbius strip.jpg , Autor = Benutzer Dbenbenn auf Commons,  
Lizenz = CC-by-sa 3.0 6
- Erläuterung: Die in diesem Text verwendeten Bilder stammen aus  
Commons (also von <http://commons.wikimedia.org>) und haben eine  
Lizenz, die die Verwendung hier erlaubt. Die Bilder werden mit ihren  
Dateinamen auf Commons angeführt zusammen mit ihrem Autor  
bzw. Hochlader und der Lizenz. 9
- Lizenzklärung: Diese Seite wurde von Holger Brenner alias  
Bocardodarapti auf der deutschsprachigen Wikiversity erstellt und  
unter die Lizenz CC-by-sa 3.0 gestellt. 9