Prof. Dr. H. Brenner **Osnabrück SS 2008**

Zahlentheorie

Vorlesung 21

Wir beschreiben nun die Ideale in einem quadratischen Zahlbereich genauer. Eine Strukturtheorie ist wichtig in Hinblick auf die Endlichkeit der Klassenzahl. Wir wissen bereits aufgrund von Korollar 18.7, dass jedes von null verschiedene Ideal von zwei Elementen über $\mathbb{Z}$ erzeugt wird. Genauer gilt.

SATZ 21.1. *(Basis für Ideale) Sei A_D ein quadratischer Zahlbereich mit Ganzheitsbasis $1, \omega$ (siehe Satz 20.9 und die daran anschließende Bemerkung) und sei $\mathfrak{a}$ ein von Null verschiedenes Ideal in A_D. Dann besitzt $\mathfrak{a}$ eine $\mathbb{Z}$-Basis aus zwei Elementen a und b, wobei $a \in \mathbb{N}$ gewählt werden kann mit $(a) = \mathbb{Z} \cap \mathfrak{a}$ und $b = \alpha + \beta\omega$ mit*

$$\beta = \min\{|\tilde{\beta}| : \tilde{\alpha} + \tilde{\beta}\omega \in \mathfrak{a},\, \tilde{\beta} \neq 0\}\,.$$

Beweis. Seien $a \in \mathbb{Z}$ und $b = \alpha + \beta\omega$ wie im Satz beschrieben gewählt. Da a und β nicht null sind folgt, dass a und b linear unabhängig über $\mathbb{Q}$ sind. Es bleibt also zu zeigen, dass jedes Element $\tilde{\alpha} + \tilde{\beta}\omega \in \mathfrak{a}$ sich als $n_1 a + n_2 b$ schreiben lässt mit $n_1, n_2 \in \mathbb{Z}$. Es gibt eine Darstellung

$$\tilde{\alpha} + \tilde{\beta}\omega = q_1 a + q_2 b = q_1 a + q_2(\alpha + \beta\omega) = q_1 a + q_2\alpha + q_2\beta\omega$$

mit $q_1, q_2 \in \mathbb{Q}$. Dann ist $\tilde{\beta} = q_2\beta$. Die Zahlen β und $\tilde{\beta}$ beschreiben beide einen ω-Koeffizient von Elementen in $\mathfrak{a}$, und β war betragsmäßig minimal gewählt, so dass q_2 ganzzahlig sein muss (alle ω-Koeffizienten bilden ein Ideal in $\mathbb{Z}$). Wir ziehen in der obigen Gleichung $q_2 b \in \mathfrak{a}$ ab und erhalten

$$q_1 a = \tilde{\alpha} + \tilde{\beta}\omega - q_2 b = \tilde{\alpha} + \tilde{\beta}\omega - q_2(\alpha + \beta\omega) = \tilde{\alpha} - q_2\alpha\,,$$

und dies gehört zu $\mathbb{Z} \cap \mathfrak{a}$. Also handelt es sich um ein ganzzahliges Vielfaches von a und somit ist auch $q_1 \in \mathbb{Z}$. □

In der soeben konstruierten $\mathbb{Z}$-Basis von $\mathfrak{a}$ können wir sowohl a als auch β positiv wählen. Der Restklassenring $A_D/\mathfrak{a}$ ist eine endliche Erweiterung des endlichen Ringes $\mathbb{Z}/(a)$, also selbst endlich. Im folgenden Diagramm sind die beiden horizontalen Abbildungen injektiv.

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & A_D \\ \downarrow & & \downarrow \\ \mathbb{Z}/(a) & \longrightarrow & A_D/\mathfrak{a}\,. \end{array}$$

Wir können die Anzahl von $A_D/\mathfrak{a}$ mittels einer $\mathbb{Z}$-Basis des Ideals ausdrücken. Wegen der surjektiven Abbildung $A_D/(a) \to A_D/\mathfrak{a}$ und aufgrund von Korollar 18.9 wissen wir, dass der Restklassenring maximal a^2 Elemente besitzt.

SATZ 21.2. *(Elemente im Restklassenring) Sei A_D ein quadratischer Zahlbereich mit $\mathbb{Z}$-Basis 1 und ω und sei $\mathfrak{a}$ ein von Null verschiedenes Ideal in A_D.*

Es sei a und $b = \alpha + \beta\omega$ eine $\mathbb{Z}$-Basis (mit a, β positiv) wie im Satz 21.1 konstruiert. Dann werden die Elemente im Restklassenring $A_D/\mathfrak{a}$ eindeutig durch die Elemente

$$\{r + s\omega : 0 \leq r < a, 0 \leq s < \beta\}$$

repräsentiert. Insbesondere besitzt der Restklassenring $a \cdot \beta$ Elemente.

Beweis. Sei $r + s\omega$ ein beliebiges Element in A_D. Durch Addition von Vielfachen von $b = \alpha + \beta\omega$ kann man erreichen, dass die zweite Komponente zwischen 0 und $\beta - 1$ liegt. Durch Addition von Vielfachen von a kann man dann erreichen, dass auch die erste Komponente zwischen 0 und $a - 1$ liegt, ohne die zweite Komponente zu verändern. Es wird also jede Restklasse durch Elemente im angegebenen Bereich repräsentiert.

Seien nun $r + s\omega$ und $\tilde{r} + \tilde{s}\omega$ im angegebenen Bereich und angenommen, dass sie das gleiche Element im Restklassenring repräsentieren. Sei $\tilde{s} \geq s$. Dann gehört die Differenz $\tilde{r} - r + (\tilde{s} - s)\omega$ zu $\mathfrak{a}$ und die zweite Komponente liegt zwischen 0 und $\beta - 1$. Aufgrund der Wahl von β muss diese Komponente null sein. Dann ist aber $\tilde{r} - r$ ein Vielfaches von a und wegen $|\tilde{r} - r| < a$ muss $\tilde{r} - r = 0$ sein, so dass also die beiden Elemente übereinstimmen und der Repräsentant eindeutig ist. □

Definition 21.3. Sei $D \neq 0, 1$ quadratfrei und A_D der zugehörige quadratische Zahlbereich. Sei $\mathfrak{a}$ ein von Null verschiedenes Ideal in A_D. Dann nennt man die (endliche) Anzahl des Restklassenringes $A_D/\mathfrak{a}$ die *Norm* von $\mathfrak{a}$. Sie wird mit

$$N(\mathfrak{a})$$

bezeichnet.

Mit der Norm lässt sich obiger Satz wie folgt ausdrücken.

Korollar 21.4. *Sei A_D ein quadratischer Zahlbereich mit $\mathbb{Z}$-Basis 1 und ω und sei $\mathfrak{a}$ ein von Null verschiedenes Ideal in A_D. Es sei a und $b = \alpha + \beta\omega$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$ (mit a, β positiv) wie im Satz 21.1 konstruiert. Dann ist*

$$N(\mathfrak{a}) = a\beta\,.$$

Beweis. Dies folgt unmittelbar aus Satz 21.2. □

Korollar 21.5. *Sei A_D ein quadratischer Zahlbereich mit $\mathbb{Z}$-Basis 1 und ω und sei $\mathfrak{a}$ ein von Null verschiedenes Ideal in A_D. Es sei $u = u_1 + u_2\omega$ und $v = v_1 + v_2\omega$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$. Dann ist*

$$N(\mathfrak{a}) = |\det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}|\,.$$

Beweis. Die Aussage ist für eine Basis der Form a und $b = \alpha + \beta\omega$, wie sie im Satz 21.1 konstruiert wurde, richtig. Für eine beliebige Basis u, v gibt es eine Übergangsmatrix M mit

$$u = Ma \text{ und } v = Mb\,.$$

Dabei ist M ganzzahlig und ihre Determinante hat den Betrag 1, so dass sich der Betrag der Determinante der Basis nicht ändert. □

Für ein Element und das davon erzeugte Hauptideal stimmen die beiden Normbegriffe überein.

SATZ 21.6. *Sei A_D ein quadratischer Zahlbereich und sei $f \neq 0$ ein Element. Setze $\mathfrak{a} = (f)$. Dann gilt $N(\mathfrak{a}) = |N(f)|$.*

Beweis. Sei $f = f_1 + f_2\omega$ mit

$$\omega = \begin{cases} \sqrt{D}, & \text{falls } D = 2,3 \mod 4 \\ \frac{1+\sqrt{D}}{2}, & \text{falls } D = 1 \mod 4\,. \end{cases}$$

Die Norm von f ist dann $N(f) = f\bar{f} =$

$$\begin{cases} (f_1 + f_2\sqrt{D})(f_1 - f_2\sqrt{D}) = f_1^2 - f_2^2 D, & D = 2,3 \mod 4 \\ (f_1 + \frac{1}{2}f_2 + \frac{f_2\sqrt{D}}{2})(f_1 + \frac{1}{2}f_2 - \frac{f_2\sqrt{D}}{2}) = (f_1 + \frac{1}{2}f_2)^2 - \frac{f_2^2}{4}D, & D = 1 \mod 4\,. \end{cases}$$

Wir berechnen nun die Norm des von f erzeugten Ideals $\mathfrak{a} = (f)$ mit Hilfe des Korollars 21.5. Eine $\mathbb{Z}$-Basis des Ideals ist offenbar gegeben durch f und $f\omega$, wobei

$$f\omega = f_1\omega + f_2\omega^2 = \begin{cases} f_2 D + f_1\omega, & \text{falls } D = 2,3 \mod 4 \\ f_2\frac{D-1}{4} + (f_1 + f_2)\omega, & \text{falls } D = 1 \mod 4\,. \end{cases}$$

Im ersten Fall haben wir

$$|\det \begin{pmatrix} f_1 & f_2 D \\ f_2 & f_1 \end{pmatrix}| = |f_1^2 - f_2^2 D|$$

und im zweiten Fall ist

$$|\det \begin{pmatrix} f_1 & f_2\frac{D-1}{4} \\ f_2 & f_1 + f_2 \end{pmatrix}| = |f_1(f_1 + f_2) - f_2^2\frac{D-1}{4}| = |f_1^2 + f_1 f_2 + \frac{1}{4}f_2^2 - \frac{1}{4}f_2^2 D|\,,$$

was mit den obigen Ergebnissen übereinstimmt. □

SATZ 21.7. *Sei A_D ein quadratischer Zahlbereich und sei $\mathfrak{a}$ ein von Null verschiedenes Ideal in A_D. Dann gilt*

$$\mathfrak{a}\bar{\mathfrak{a}} = (N(\mathfrak{a}))\,.$$

Beweis. Sei $\mathfrak{a}$ durch eine $\mathbb{Z}$-Basis $a, b = \alpha + \beta\omega$ wie im Satz 21.1 gegeben. Das konjugierte Ideal $\bar{\mathfrak{a}}$ hat die Basis a und $\bar{b}$. Das Produktideal $\mathfrak{a}\bar{\mathfrak{a}}$ hat die vier Erzeuger

$$a^2, N(b), a\bar{b}, ab\,.$$

Wir behaupten, dass dieses Ideal gleich dem von $(a\beta)$ erzeugten Ideal ist, was ja nach Korollar 21.4 die Norm von $\mathfrak{a}$ ist. Zunächst teilt β sowohl a als auch α: Wegen $a\omega \in \mathfrak{a}$ hat man nämlich eine Darstellung

$$a\omega = \gamma a + \delta(\alpha + \beta\omega)$$

mit $\gamma, \delta \in \mathbb{Z}$. Daraus folgt durch Koeffizientenvergleich $a = \delta\beta$ und andererseits $\gamma a + \delta\alpha = 0$, woraus nach Kürzen mit δ sich $\alpha = -\gamma\beta$ ergibt. Insbesondere ist

$$\mathfrak{a} = (a, \alpha + \beta\omega) = (\beta\delta, -\beta\gamma + \beta\omega) = (\beta)(\delta, -\gamma + \omega)\,.$$

Mit dem Ideal $\mathfrak{b} = (\delta, -\gamma + \omega)$ können wir wegen $\mathfrak{a}\bar{\mathfrak{a}} = (\beta^2)\mathfrak{b}\bar{\mathfrak{b}}$ und wegen $N(\mathfrak{a}) = a\beta = \delta\beta^2 = \beta^2 N(\mathfrak{b})$ annehmen, dass $\beta = 1$ ist.

In dieser neuen Situation müssen wir $\mathfrak{a}\bar{\mathfrak{a}} = (a)$ zeigen. Aufgrund von $N(b) \in \mathfrak{a} \cap \mathbb{Z} = (a)$ haben wir die Inklusion $\mathfrak{a}\bar{\mathfrak{a}} \subseteq (a)$. Wir betrachten die Inklusionskette (in A_D)

$$(a^2, N(b), a(b + \bar{b})) \subseteq (a^2, N(b), ab, a\bar{b}) = \mathfrak{a}\bar{\mathfrak{a}} \subseteq (a)\,.$$

Es sei $c \in \mathbb{Z}$ der Erzeuger des Ideals links. Wir behaupten zunächst, dass die linke Inklusion eine Gleichheit ist. Dafür betrachten wir die Norm und die Spur von ab/c und erhalten

$$N(\frac{ab}{c}) = \frac{N(a)N(b)}{N(c)} = \frac{a^2 N(b)}{c^2} \in \mathbb{Z}\,.$$

und

$$S(\frac{ab}{c}) = \frac{1}{c}S(ab) = \frac{1}{c}(ab + a\bar{b}) \in \mathbb{Z}\,.$$

Damit sind die Norm und die Spur ganz über $\mathbb{Z}$, nach Lemma 20.8 ist das Element selbst ganz und damit ist ab ein Vielfaches von c. Wir wissen also

$$\frac{ab}{c} = \frac{a(\alpha + \omega)}{c} = \frac{\alpha}{c}a + \frac{a}{c}\omega \in A_D$$

und damit ist $\frac{a}{c} \in \mathbb{Z}$. Also wird a von c geteilt und in der Inklusionskette gilt Gleichheit. □

Korollar 21.8. *(Multiplikativität der Norm) Sei A_D ein quadratischer Zahlbereich und seien $\mathfrak{a}$ und $\mathfrak{b}$ von Null verschiedene Ideale in A_D. Dann gilt*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})\,.$$

Beweis. Wir wenden Satz 21.7 wiederholt für Ideale an und erhalten

$$(N(\mathfrak{ab})) = (\mathfrak{ab})\overline{(\mathfrak{ab})} = \mathfrak{ab}\bar{\mathfrak{a}}\bar{\mathfrak{b}} = \mathfrak{a}\bar{\mathfrak{a}}\mathfrak{b}\bar{\mathfrak{b}} = (N(\mathfrak{a}))(N(\mathfrak{b})) = (N(\mathfrak{a})N(\mathfrak{b}))\,.$$

Da die Norm eines Ideals stets positiv ist folgt aus dieser Idealidentität die Gleichheit $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$. □