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

Zahlentheorie

Vorlesung 21

Ideale und ihre Norm in einem quadratischen Zahlbereich

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 18.9, dass jedes von 0 verschiedene Ideal von zwei Elementen über $\mathbb{Z}$ erzeugt wird. Genauer gilt.

SATZ 21.1. *Sei A_D ein quadratischer Zahlbereich mit Ganzheitsbasis $1, \omega$ (im Sinne von Satz 20.9) und sei $\mathfrak{a}$ ein von 0 verschiedenes Ideal in A_D. Dann besitzt $\mathfrak{a}$ eine $\mathbb{Z}$-Basis aus zwei Elementen a und b, wobei $a \in \mathbb{N}$ mit $(a) = \mathbb{Z} \cap \mathfrak{a}$ und*

$$b = \alpha + \beta\omega$$

mit

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

gewählt werden kann.

Beweis. Seien $a \in \mathbb{N}$ und $b = \alpha + \beta\omega$ wie im Satz beschrieben gewählt. Da a und β nicht 0 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 $n_1 a + n_2 b$ mit $n_1, n_2 \in \mathbb{Z}$ schreiben lässt. 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-Koeffizienten 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.

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

Wegen der surjektiven Abbildung $A_D/(a) \to A_D/\mathfrak{a}$ und aufgrund von Korollar 18.11 wissen wir, dass der Restklassenring maximal a^2 Elemente besitzt.

Beispiel 21.2. Wir betrachten im quadratischen Zahlbereich R zu $D = -5$ das Ideal

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

Da es sich nicht um das Einheitsideal handelt, ist unmittelbar klar, dass bereits eine $\mathbb{Z}$-Basis im Sinne von Satz 21.1 vorliegt. Die Norm dieses Ideals ist 2. Die Normen der beiden Elemente sind

$$N(2) = 4$$

und

$$N(1 + \sqrt{-5}) = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6.$$

Satz 21.3. *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 0 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 21.4. Sei $D \neq 0, 1$ quadratfrei und A_D der zugehörige quadratische Zahlbereich. Sei $\mathfrak{a}$ ein von 0 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 21.5. *Sei A_D ein quadratischer Zahlbereich mit $\mathbb{Z}$-Basis 1 und ω und sei $\mathfrak{a}$ ein von 0 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 21.3. □

KOROLLAR 21.6. *Sei A_D ein quadratischer Zahlbereich mit $\mathbb{Z}$-Basis 1 und ω und sei $\mathfrak{a}$ ein von 0 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*

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

Beweis. Die Aussage ist für eine $\mathbb{Z}$-Basis der Form a und $b = \alpha + \beta\omega$, wie sie im Satz 21.1 konstruiert wurde, richtig. Für eine beliebige $\mathbb{Z}$-Basis u, v gibt es eine Übergangsmatrix M mit $u = Ma$ 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 21.7. *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

$$\begin{array}{rcl} N(f) & = & f\overline{f} \\ & = & \begin{cases} \left(f_1 + f_2\sqrt{D}\right)\left(f_1 - f_2\sqrt{D}\right) = f_1^2 - f_2^2 D, & \text{falls } D = 2,3 \mod 4, \\ \left(f_1 + \frac{1}{2}f_2 + \frac{f_2\sqrt{D}}{2}\right)\left(f_1 + \frac{1}{2}f_2 - \frac{f_2\sqrt{D}}{2}\right) = \left(f_1 + \frac{1}{2}f_2\right)^2 - \frac{f_2^2}{4}D, & \text{falls } D = 1 \mod 4. \end{cases} \end{array}$$

Wir berechnen nun die Norm des von f erzeugten Ideals $\mathfrak{a} = (f)$ mit Hilfe von Korollar 21.6. Eine $\mathbb{Z}$-Basis des Ideals ist offenbar gegeben durch f und $f\omega$, wobei

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

ist. Im ersten Fall haben wir

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

und im zweiten Fall ist

$$\begin{aligned}\left|\det\begin{pmatrix} f_1 & f_2\frac{D-1}{4} \\ f_2 & f_1+f_2 \end{pmatrix}\right| &= \left|f_1(f_1+f_2)-f_2^2\frac{D-1}{4}\right| \\ &= \left|f_1^2+f_1f_2+\frac{1}{4}f_2^2-\frac{1}{4}f_2^2D\right|,\end{aligned}$$

was mit den obigen Ergebnissen übereinstimmt. □

Beispiel 21.8. Wir betrachten im quadratischen Zahlbereich R zu $D=-5$ das Ideal

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

Wir behaupten, dass es kein Hauptideal ist und verwenden dabei, dass die Norm dieses Ideals gleich 2 ist. Wäre nämlich $\mathfrak{p}=(f)$ mit einem $f \in R$, so müsste nach Satz 21.7 auch

$$|N(f)| = 2$$

gelten. Allerdings ist die Norm von $f=a+b\sqrt{-5}$ gleich $N(f)=a^2+5b^2$ und dies kann nicht gleich 2 sein.

Beispiel 21.9. Wir betrachten im quadratischen Zahlbereich R zu $D=-5$ das Ideal $\mathfrak{p}=(2,1+\sqrt{-5})$, das nach Beispiel 21.8 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 da 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

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

$$\begin{aligned} &= \sqrt{2}(-2+3) \\ &= \sqrt{2}. \end{aligned}$$

SATZ 21.10. *Sei A_D ein quadratischer Zahlbereich und sei $\mathfrak{a}$ ein von 0 verschiedenes Ideal in A_D. Dann gilt*

$$\mathfrak{a}\overline{\mathfrak{a}} \;=\; (N(\mathfrak{a})).$$

Beweis. Sei $\mathfrak{a}$ durch eine $\mathbb{Z}$-Basis $a, b = \alpha + \beta\omega$ wie im Satz 21.1 gegeben. Das konjugierte Ideal $\overline{\mathfrak{a}}$ hat die Basis a und $\bar{b}$. Das Produktideal $\mathfrak{a}\overline{\mathfrak{a}}$ 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 21.5 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 einerseits $a \;=\; \delta\beta$ 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

$$\mathfrak{a}\overline{\mathfrak{a}} \;=\; (\beta^2)\mathfrak{b}\overline{\mathfrak{b}}$$

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 $\mathfrak{a}\overline{\mathfrak{a}} \;\subseteq\; (a)$. Wir betrachten die Inklusionskette (in A_D)

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

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 $\frac{ab}{c}$ und erhalten

$$N\left(\frac{ab}{c}\right) \;=\; \frac{N(a)N(b)}{N(c)} \;=\; \frac{a^2 N(b)}{c^2} \;\in\; \mathbb{Z}$$

und

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

Damit gehören die Norm und die Spur zu $\mathbb{Z}$ und damit ist nach Lemma 20.8 das Element selbst ganz und somit 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 21.11. *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 21.10 wiederholt für Ideale an und erhalten

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

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

Die obige Definition der Norm eines Ideals, die wir nur für quadratische Zahlbereiche gefasst haben, lässt sich auf beliebige Zahlbereiche erweitern. Dafür gelten entsprechende Eigenschaften, was wir im Rahmen dieser Vorlesung nicht ausführen werden.

Definition 21.12. Zu einem Ideal $\mathfrak{a} \neq 0$ in einem Zahlbereich R heißt die (endliche) Anzahl des Restklassenringes $R/\mathfrak{a}$ die *Norm* von $\mathfrak{a}$. Sie wird mit

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

bezeichnet.