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

Zahlentheorie

Vorlesung 18

Wir werden uns in dieser Vorlesung hauptsächlich für den ganzen Abschluss von $\mathbb{Z}$ in einem endlichen Erweiterungskörper der rationalen Zahlen $\mathbb{Q}$ interessieren.

DEFINITION 18.1. Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung. Dann nennt man den ganzen Abschluss von $\mathbb{Z}$ in L den *Ring der ganzen Zahlen* in L. Solche Ringe nennt man auch *Zahlbereiche*.

Den endlichen Erweiterungskörper L von $\mathbb{Q}$ nennt man übrigens einen *Zahlkörper*.

SATZ 18.2. *Sei R ein Zahlbereich. Dann ist R ein normaler Integritätsbereich.*

Beweis. Nach Satz 17.13 ist L der Quotientenkörper des Ganzheitsrings R. Ist $q \in Q(R) = L$ ganz über R, so ist q nach Aufgabe 17.3 auch ganz über $\mathbb{Z}$ und gehört selbst zu R. □

LEMMA 18.3. *Sei R ein Zahlbereich. Dann enthält jedes von null verschiedene Ideal $\mathfrak{a}$ in R eine Zahl $m \in \mathbb{Z}$ mit $m \neq 0$.*

Beweis. Sei $0 \neq f \in \mathfrak{a}$. Dieses Element ist nach der Definition eines Zahlbereiches ganz über $\mathbb{Z}$ und erfüllt demnach eine Ganzheitsgleichung

$$f^n + k_{n-1}f^{n-1} + k_{n-2}f^{n-2} + \ldots + k_1 f + k_0 = 0$$

mit ganzen Zahlen k_i. Bei $k_0 = 0$ kann man die Gleichung mit f kürzen, da $f \neq 0$ ein Nichtnullteiler ist. So kann man sukzessive fortfahren und erhält schließlich eine Ganzheitsgleichung, bei der der konstante Term nicht 0 ist. Sei also in obiger Gleichung $k_0 \neq 0$. Dann ist

$$f(f^{n-1} + k_{n-1}f^{n-2} + k_{n-2}f^{n-3} + \ldots + k_1) = -k_0$$

und somit ist $k_0 \in (f) \cap \mathbb{Z}$. □

SATZ 18.4. *Sei R ein Zahlbereich und sei $f \in Q(R) = L$. Dann ist f genau dann ganz über $\mathbb{Z}$, wenn die Koeffizienten des Minimalpolynoms von f über $\mathbb{Q}$ alle ganzzahlig sind.*

Beweis. Das Minimalpolynom P von f über $\mathbb{Q}$ ist ein normiertes irreduzibles Polynom mit Koeffizienten aus $\mathbb{Q}$. Wenn die Koeffizienten sogar ganzzahlig sind, so liegt direkt eine Ganzheitsgleichung für f über $\mathbb{Z}$ vor.

Sei umgekehrt f ganz über $\mathbb{Z}$, und sei $S \in \mathbb{Z}[X]$ ein normiertes ganzzahliges Polynom mit $S(f) = 0$, das wir als irreduzibel in $\mathbb{Z}[X]$ annehmen dürfen. Wir betrachten $S \in \mathbb{Q}[X]$. Dort gilt

$$S = PT\,.$$

Da nach dem Lemma von Gauß (siehe Aufgabe 18.2) ein irreduzibles Polynom von $\mathbb{Z}[X]$ auch in $\mathbb{Q}[X]$ irreduzibel ist, folgt $S = P$ und daher sind alle Koeffizienten von P ganzzahlig. □

Es ergibt sich insbesondere, dass die Norm und die Spur von Elementen aus einem Zahlbereich zu $\mathbb{Z}$ gehören.

LEMMA 18.5. *Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Sei $\mathfrak{a}$ ein von null verschiedenes Ideal in R. Dann enthält $\mathfrak{a}$ Elemente $b_1, \ldots, b_n$, die eine $\mathbb{Q}$-Basis von L sind.*

Beweis. Es sei $v_1, \ldots, v_n$ eine $\mathbb{Q}$-Basis von L. Das Ideal $\mathfrak{a}$ enthält nach Lemma 18.3 ein Element $0 \neq m \in \mathfrak{a} \cap \mathbb{Z}$. Nach (dem Beweis von) Satz 17.13 kann man schreiben $v_i = \frac{r_i}{n_i}$ mit $r_i \in R$ und $n_i \in \mathbb{Z} - \{0\}$. Dann sind die $m(n_i v_i) \in \mathfrak{a}$ und bilden ebenfalls eine $\mathbb{Q}$-Basis von L. □

SATZ 18.6. *Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Sei $\mathfrak{a}$ ein von null verschiedenes Ideal in R. Seien $b_1, \ldots, b_n \in \mathfrak{a}$ Elemente, die eine $\mathbb{Q}$-Basis von L bilden und für die der Betrag der Diskriminante*

$$|\triangle(b_1, \ldots, b_n)|$$

unter all diesen Basen aus $\mathfrak{a}$ minimal sei. Dann ist

$$\mathfrak{a} = \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n \,.$$

Beweis. Sei $f \in \mathfrak{a}$ ein beliebiges Element. Wir haben zu zeigen, dass sich f als eine $\mathbb{Z}$-Linearkombination $f = k_1 b_1 + \ldots + k_n b_n$ mit $k_i \in \mathbb{Z}$ schreiben lässt, wenn die $b_1, \ldots, b_n \in \mathfrak{a}$ eine $\mathbb{Q}$-Basis von L mit minimalem Diskriminantenbetrag bilden. Es gibt eine eindeutige Darstellung

$$f = q_1 b_1 + \ldots + q_n b_n$$

mit rationalen Zahlen $q_i \in \mathbb{Q}$. Sei angenommen, dass ein q_i nicht ganzzahlig ist, wobei wir $i = 1$ annehmen dürfen. Wir schreiben dann $q_1 = k + \delta$ mit $k \in \mathbb{Z}$ und einer rationalen Zahl δ zwischen 0 und 1. Dann ist auch

$$c_1 = f - kb_1 = \delta b_1 + \sum_{i=2}^{n} q_i b_i,\ b_2, \ldots, b_n$$

eine $\mathbb{Q}$-Basis von L, die in $\mathfrak{a}$ liegt. Die Übergangsmatrix der beiden Basen ist

$$T = \begin{pmatrix} \delta & q_2 & q_3 & \cdots & q_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} .$$

Nach Lemma 16.2 gilt für die beiden Diskriminanten die Beziehung

$$\triangle(c_1, b_2, \ldots, b_n) = (\det(T))^2 \triangle(b_1, b_2, \ldots, b_n) \,.$$

Wegen $= (\det(T))^2 = \delta^2 < 1$ und da die Diskriminanten nach Lemma 16.3 nicht null sind, ist dies ein Widerspruch zur Minimalität der Diskriminanten. □

KOROLLAR 18.7. *(Struktur von Idealen) Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Sei $\mathfrak{a}$ ein von null verschiedenes Ideal in R. Dann ist $\mathfrak{a}$ eine freie Gruppe vom Rang n, d.h. es gibt Elemente $b_1, \ldots, b_n \in \mathfrak{a}$ mit*

$$\mathfrak{a} = \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n \, .$$

Beweis. Nach Lemma 18.5 gibt es überhaupt Elemente $b_1, \ldots, b_n \in \mathfrak{a}$, die eine $\mathbb{Q}$-Basis von L bilden. Daher gibt es auch solche Basen, wo der Betrag der Diskriminante minimal ist. Für diese gilt nach Satz 18.6, dass sie ein $\mathbb{Z}$-Erzeugendensystem von $\mathfrak{a}$ bilden. □

KOROLLAR 18.8. *(Additive Struktur der Zahlbereiche) Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Dann ist R eine freie Gruppe vom Rang n, d.h. es gibt Elemente $b_1, \ldots, b_n \in R$ mit*

$$R = \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n \, .$$

Beweis. Dies folgt direkt aus Korollar 18.7, angewendet auf das Ideal $\mathfrak{a} = R$. □

Ein solches System von Erzeugern $b_1, \ldots, b_n$ nennt man auch eine *Ganzheitsbasis*.

KOROLLAR 18.9. *Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Es sei $m \in \mathbb{Z}$. Dann gibt es einen Gruppenisomorphismus*

$$R/(m) \cong (\mathbb{Z}/(m))^n \, .$$

Für eine Primzahl $m = p$ ist $R/(m)$ eine Algebra der Dimension n über dem Körper $\mathbb{Z}/(p)$. Zu jeder Primzahl p gibt es Primideale $\mathfrak{p}$ in R mit $\mathfrak{p} \cap \mathbb{Z} = (p)$.

Beweis. Nach Korollar 18.8 ist $R \cong \mathbb{Z}^n$ (als abelsche Gruppen). Das von m in R erzeugte Ideal besteht (unter dieser Identifizierung) aus allen Elementen der Form

$$m(a_1, \ldots, a_n) = (ma_1, \ldots, ma_n) \, ,$$

d.h. in jeder Komponente steht ein Vielfaches von m. Die Restklassengruppe $R/(m)$ ist demnach gleich $(\mathbb{Z}/(m))^n$ und besitzt m^n Elemente. Aufgrund der Ganzheit ist $mR \cap \mathbb{Z} = m\mathbb{Z}$ (siehe Aufgabe 18.4) und aufgrund des Isomorphiesatzes hat man einen injektiven Ringhomomorphismus

$$\mathbb{Z}/(m) \longrightarrow R/(m) \, ,$$

so dass $R/(m)$ eine von null verschiedene $\mathbb{Z}/(m)$-Algebra ist.

Für eine Primzahl p ist $R/(p)$ ein Vektorraum über $\mathbb{Z}/(p)$ der Dimension n. Deshalb gibt es darin (mindestens) ein maximales Ideal, und dieses entspricht einem maximalen Ideal $\mathfrak{m}$ in R mit $p \in \mathfrak{m}$. Daher ist $(p) = (p)R \cap \mathbb{Z} \subseteq \mathfrak{m} \cap \mathbb{Z}$, und dieser Durchschnitt ist ein Primideal, also gleich (p). □

Emmy Noether (1882-1935)

DEFINITION 18.10. Ein kommutativer Ring R heißt *noethersch*, wenn jedes Ideal darin endlich erzeugt ist.

KOROLLAR 18.11. *(Zahlbereiche sind noethersch) Jeder Zahlbereich ist ein noetherscher Ring.*

Beweis. Nach Satz 18.6 ist jedes von null verschiedene Ideal als additive Gruppe isomorph zu $\mathbb{Z}^n$, also ist insbesondere jedes Ideal als abelsche Gruppe endlich erzeugt. Insbesondere sind die Ideale dann als Ideale (also als R-Moduln) endlich erzeugt. □

SATZ 18.12. *Sei R ein Zahlbereich. Dann ist jeder echte Restklassenring von R endlich.*

Beweis. Nach 18.3 gibt es ein $m \in \mathbb{Z} \cap \mathfrak{a}$, $m \neq 0$. Damit ist $mR \subseteq \mathfrak{a}$ und damit hat man eine surjektive Abbildung

$$R/(m) \longrightarrow R/\mathfrak{a}\,.$$

Der Ring links ist nach 18.9 endlich (mit m^n Elementen), also besitzt der Ring rechts auch nur endlich viele Elemente. □

SATZ 18.13. *Sei R ein Zahlbereich. Dann ist jedes von null verschiedene Primideal von R bereits ein maximales Ideal.*

Beweis. Sei $\mathfrak{p}$ ein Primideal $\neq 0$ in R. Dann ist der Restklassenring $R/\mathfrak{p}$ nach Lemma 16.13 ein Integritätsbereich und nach Satz 18.12 endlich. Ein endlicher Integritätsbereich ist aber bereits ein Körper, so dass nach Satz 18.12 ein maximales Ideal vorliegt. □

Richard Dedekind (1831-1916)

Die bisher etablierten Eigenschaften von Zahlbereichen lassen sich im folgenden Begriff zusammenfassen.

DEFINITION 18.14. Einen Integritätsbereich R nennt man einen *Dedekindbereich*, wenn er noethersch und normal ist und wenn jedes von null verschiedene Primideal darin maximal ist.

KOROLLAR 18.15. *(Zahlbereiche sind Dedekindbereiche) Jeder Zahlbereich ist ein Dedekindbereich.*

Beweis. Dies folgt aus Satz 18.2, aus Korollar 18.11 und aus Satz 18.13. □

Abbildungsverzeichnis