Prof. Dr. H. Brenner **Osnabrück WS 2020/2021**

Algebraische Zahlentheorie

Vorlesung 7

Zahlbereiche

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

DEFINITION 7.1. Es 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*. Diese Zahlbereiche sind der Gegenstand der algebraischen Zahlentheorie. Wir interessieren uns in der algebraischen Zahlentheorie insbesondere für folgende Fragen.

(1) Wann ist ein Zahlbereich R ein Hauptidealbereich und wann ist er faktoriell?
(2) Wenn R kein Hauptidealbereich ist, gibt es dann andere Versionen, die die eindeutige Primfaktorzerlegung ersetzen? (Ja: Lokal und auf Idealebene, siehe Korollar 10.17, Satz 10.17, Bemerkung 10.9 einerseits und Satz 12.2 andererseits.)
(3) Wenn R kein Hauptidealbereich ist, kann man dann die Abweichung von der Eigenschaft, ein Hauptidealbereich zu sein, in irgendeiner Form messen? (Ja: Durch die sogenannte Klassengruppe. Siehe Satz 14.2 und Satz 26.6.)
(4) Was passiert mit den Primzahlen in den Zahlbereichen? Gibt es eine Regelmäßigkeit, wie diese in R zerlegt werden? (siehe Korollar 8.8.)
(5) Was kann man über die Einheiten in einem Zahlbereich sagen? (Siehe Satz 28.7.)
(6) Inwiefern reflektieren Eigenschaften von Zahlbereichen Eigenschaften der ganzen Zahlen selbst?

SATZ 7.2. *Sei R ein Zahlbereich. Dann ist R ein normaler Integritätsbereich.*

Beweis. Nach Lemma 6.16 ist L der Quotientenkörper des Ganzheitsrings R. Ist $q \in Q(R) = L$ ganz über R, so ist q nach Aufgabe 6.22 auch ganz über $\mathbb{Z}$ und gehört selbst zu R. □

Ein Ganzheitsring ist im Allgemeinen nicht faktoriell.

LEMMA 7.3. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und es sei $R \subseteq L$ ein Unterring mit den folgenden Eigenschaften:*

(1) *R ist ganz über $\mathbb{Z}$.*
(2) *Es ist $Q(R) = L$.*
(3) *R ist normal.*

Dann ist R der Ring der ganzen Zahlen von L.

Beweis. Siehe Aufgabe 7.1. □

Beispiel 7.4. Wir betrachten die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{-3}]$, der die Ringe

$$\mathbb{Z}[\sqrt{-3}] = A \subseteq \mathbb{Z}[\omega] = B \subseteq \mathbb{Q}[\sqrt{-3}]$$

enthält, wobei $\omega = -\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3}$ ist, d.h. $\mathbb{Z}[\omega]$ ist der Ring der Eisenstein-Zahlen. Der Quotientenkörper von beiden Ringen ist $\mathbb{Q}[\sqrt{-3}]$. Das Element ω erfüllt die Ganzheitsgleichung

$$\omega^2 + \omega + 1 = 0,$$

und somit ist $\mathbb{Z}[\omega]$ ganz über $\mathbb{Z}$. Ferner ist $\mathbb{Z}[\omega]$ normal. Dies ergibt sich aus Satz Anhang 2.7, Satz Anhang 2.8, Satz 2.19 und Satz 6.12. Nach Lemma 7.3 ist also insgesamt der Ring der Eisenstein-Zahlen der Ring der ganzen Zahlen in $\mathbb{Q}[\sqrt{-3}]$.

Satz 7.5. *Es 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 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. □

Ideale in Zahlbereichen

In $\mathbb{Z}[\mathrm{i}]$ ist jedes Ideal ein Hauptideal und es ist

$$(a + b\mathrm{i}) = \{m(a + b\mathrm{i}) + n\mathrm{i}(a + b\mathrm{i}) \mid m, n \in \mathbb{Z}\} \cong \mathbb{Z}^2$$

(die letzte Gleichung setzt voraus, dass es sich nicht um das Nullideal handelt). Eine ähnlich einfache Gruppenstruktur gilt für jedes Ideal in einem Zahlbereich, was wir in Korollar 8.5 beweisen werden.

LEMMA 7.6. *Es sei R ein Zahlbereich. Dann enthält jedes von 0 verschiedene Ideal $\mathfrak{a} \subseteq R$ 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

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

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

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

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

LEMMA 7.7. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Sei $\mathfrak{a}$ ein von 0 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 7.6 ein Element $0 \neq m \in \mathfrak{a} \cap \mathbb{Z}$. Nach (dem Beweis von) Lemma 6.16 kann man $v_i = \frac{r_i}{n_i}$ mit $r_i \in R$ und $n_i \in \mathbb{Z} \setminus \{0\}$ schreiben. Dann sind die $m(n_i v_i) \in \mathfrak{a}$ und sie bilden ebenfalls eine $\mathbb{Q}$-Basis von L. □

Spur und Norm

Zu einer R-Algebra S definiert jedes Element $f \in S$ einen R-Modulhomomorphismus $S \to S$, $x \mapsto fx$, die *Multiplikationsabbildung*. Wenn S eine endlich erzeugte freie R-Algebra ist, ihre additive Struktur also die Form $S = R^n$ besitzt, so wird dieser Multiplikationshomomorphismus bezüglich einer R-Basis von S durch eine $n \times n$-Matrix beschrieben, die die *Multiplikationsmatrix* (zu f bezüglich dieser Basis) heißt. In diesem Fall kann man Konzepte der Matrixtheorie der linearen Algebra auf diese Multiplikationsabbildung anwenden. Diese Situation liegt bei einer endlichen Körpererweiterung $K \subseteq L$ vor, aber auch ein Zahlbereich ist stets nach Korollar 8.6 eine freie $\mathbb{Z}$-Algebra. Aber auch wenn $R \subseteq S$ Integritätsbereiche sind mit S endlich erzeugt als R-Modul, so kann man auch im nichtfreien Fall über die Quotientenkörper die folgenden Konzepte anwenden.

DEFINITION 7.8. Es sei R ein kommutativer Ring und sei S eine kommutative endliche freie R-Algebra. Zu einem Element $f \in S$ nennt man die Spur des R-Modulhomomorphismus

$$\mu_f \colon S \longrightarrow S,\ y \longmapsto fy,$$

die *Spur* von f. Sie wird mit $\operatorname{Spur}(f)$ bezeichnet.

Definition 7.9. Es sei R ein kommutativer Ring und sei S eine kommutative endliche freie R-Algebra. Zu einem Element $f \in S$ nennt man die Determinante des R-Modulhomomorphismus

$$\mu_f \colon S \longrightarrow S,\, y \longmapsto fy,$$

die *Norm* von f. Sie wird mit $N(f)$ bezeichnet.

Bei einer freien R-Algebra S ist die Spur

$$S \longrightarrow R,\, f \longmapsto \operatorname{Spur}(f),$$

R-linear und insbesondere additiv und die Norm

$$S \longrightarrow R,\, f \longmapsto N(f),$$

ist multiplikativ. Darin liegen ihre jeweiligen Bedeutungen, dass mit ihrer Hilfe additive bzw. multiplikative Eigenschaften von S in R widergespiegelt werden können. Einen Ringhomomorphismus von S nach R gibt es nur sehr selten, deshalb sind Spur und Norm in gewissem Sinne optimal.

Die Interpretation eines Elementes als lineare Abbildung hilft auch dabei, das Minimalpolynom zu bestimmen.

Lemma 7.10. *Es sei $K \subseteq L$ eine endliche Körpererweiterung und $f \in L$ ein Element mit der Multiplikationsabbildung*

$$\mu_f \colon L \longrightarrow L,\, y \longmapsto fy.$$

Dann ist in $K[X]$ das charakteristische Polynom von μ_y ein Vielfaches des Minimalpolynoms von f. Bei $L = K[f]$ stimmt das charakteristische Polynom mit dem Minimalpolynom überein.

Beweis. Die Zuordnung

$$L \longrightarrow \operatorname{End}(L),\, f \longmapsto \mu_f,$$

ist ein injektiver Ringhomomorphismus. Es sei χ das charakteristische Polynom von μ_f. Nach Cayley-Hamilton ist

$$\chi(\mu_f) = 0$$

im Endomorphismenring. Damit ist auch

$$\chi(f) = 0$$

in $K[X]$. Nach Satz 2.12 ist somit das Minimalpolynom ein Teiler des charakteristischen Polynoms. Bei $L = K[f]$ besitzt das Minimalpolynom und das charakteristische Polynom den gleichen Grad, also stimmen sie überein. □

Da wir noch nicht gezeigt haben, dass Zahlbereiche frei sind, verwenden wir Spur und Norm über die Quotientenkörper. Allerdings können wir hier schon begründen, dass die Spur und die Norm eines ganzen Elementes zum Grundring gehört.

Korollar 7.11. *Es sei R ein Zahlbereich und sei $f \in R$. Dann ist die Spur und die Norm von f ganzzahlig.*

Beweis. Eine Verfeinerung der Argumentation zu Lemma 7.10 zeigt, dass das charakteristische Polynom zu f eine Potenz des Minimalpolynoms zu f ist. Da nach Satz 7.5 die Koeffizienten des Minimalpolynoms ganzzahlig sind, überträgt sich dies auf das charakteristische Polynom. Spur und Norm treten aber nach Aufgabe 7.17 und Aufgabe 7.18 als Koeffizienten des charakteristischen Polynoms auf. □

Einbettungen in die komplexen Zahlen

Satz 7.12. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n. Dann gibt es genau n Einbettungen von L in die komplexen Zahlen $\mathbb{C}$.*

Beweis. Nach dem Satz vom primitiven Element wird L durch ein Element erzeugt, es ist also

$$L = \mathbb{Q}(x) \cong \mathbb{Q}[X]/(F)$$

mit einem irreduziblen Polynom $F \in \mathbb{Q}[X]$ vom Grad n. Da F irreduzibel ist und da die Ableitung $F' \neq 0$ ist und kleineren Grad besitzt, folgt, dass F und F' teilerfremd sind. Nach Satz 2.12 ergibt sich, dass F und F' das Einheitsideal erzeugen, also $AF + BF' = 1$ ist. Wir betrachten diese Polynome nun als Polynome in $\mathbb{C}[X]$, wobei die polynomialen Identitäten erhalten bleiben. Über den komplexen Zahlen zerfallen F und F' in Linearfaktoren, und wegen der Teilerfremdheit bzw. der daraus resultierenden Identität haben F und F' keine gemeinsame Nullstelle. Daraus folgt wiederum, dass F keine mehrfache Nullstelle besitzt, sondern genau n verschiedene komplexe Zahlen $z_1, \ldots, z_n$ als Nullstellen besitzt. Jedes z_i definiert nun einen Ringhomomorphismus

$$\rho_i \colon L \cong \mathbb{Q}[X]/(F) \longrightarrow \mathbb{C},\ X \longmapsto z_i.$$

Da L ein Körper ist, ist diese Abbildung injektiv. Da dabei X auf verschiedene Elemente abgebildet wird, liegen n verschiedene Abbildungen vor. Es kann auch keine weiteren Ringhomomorphismen $L \to \mathbb{C}$ geben, da jeder solche durch $X \mapsto z$ gegeben ist und $F(z) = 0$ sein muss. □

Statt von komplexen Einbettungen spricht man auch von komplexen Realisierungen. Man beachte im vorstehenden Satz, dass das Bild von verschiedenen Einbettungen

$$\rho_i \colon L \longrightarrow \mathbb{C}$$

der gleiche Unterkörper von $\mathbb{C}$ sein kann. Dies gilt bereits für quadratische Erweiterungen wie $\mathbb{Q}[\mathrm{i}]$. Man hat die beiden Einbettung $\rho_1, \rho_2 \colon \mathbb{Q}[\mathrm{i}] \to \mathbb{C}$, wobei die eine Abbildung i auf i und die andere i auf $-\mathrm{i}$ schickt. Das Bild ist aber in beiden Fällen gleich.

Wenn das Bild einer Einbettung ganz in den reellen Zahlen liegt, so spricht man auch von einer *reellen Einbettung*. Die Anzahl der reellen Einbettungen und die Anzahl der imaginären Einbettungen spielt eine wichtige Rolle in der algebraischen Zahlentheorie. Zu einem Element $z \in L$ nennt man die verschiedenen komplexen Zahlen

$$z_1 = \rho_1(z), \ldots, z_n = \rho_n(z)$$

zueinander konjugiert. Diese sind allesamt Nullstellen eines irreduziblen Polynoms F mit rationalen Koeffizienten vom Grad n.

LEMMA 7.13. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und $z \in L$ ein Element. Es seien*

$$\rho_1, \ldots, \rho_n \colon L \longrightarrow \mathbb{C}$$

die verschiedenen komplexen Einbettungen und es sei $M = \{y_1, \ldots, y_k\}$ die Menge der verschiedenen Werte $\rho_i(z)$. Dann gilt in $\mathbb{C}[X]$ für das Minimalpolynom G von z die Gleichung

$$G = (X - y_1)(X - y_2) \cdots (X - y_k).$$

Beweis. Es sei $K \subseteq L$ der von z erzeugte Unterkörper von L. Es ist dann

$$K \cong \mathbb{Q}[X]/(G)$$

mit dem (normierten) Minimalpolynom G von z und K (bzw. G) haben den Grad m über $\mathbb{Q}$. Gemäß Satz 7.12 gibt es m Einbettungen $\sigma \colon K \to \mathbb{C}$, die den komplexen Nullstellen M' von G entsprechen, und daher ist

$$G = \prod_{\sigma} (X - \sigma(z)).$$

Die n Einbettungen $\rho_i \colon L \to \mathbb{C}$ induzieren jeweils eine Einbettung

$$\sigma_i = \rho_i|_K \colon K \longrightarrow \mathbb{C}$$

und somit ist $\rho_i(z) = \sigma_i(z)$, also $M \subseteq M'$. Andererseits lässt sich eine Einbettung $\sigma \colon K \to \mathbb{C}$ zu einer Einbettung $L \to \mathbb{C}$ fortsetzen, da L über K separabel ist und nach dem Satz vom primitiven Element von einem Element erzeugt wird und das zugehörige Minimalpolynom über $\mathbb{C}$ zerfällt. Daher ist auch $M' \subseteq M$. □

LEMMA 7.14. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $\rho_i \colon L \to \mathbb{C}$ die n verschiedenen komplexen Einbettungen. Es sei $z \in L$ und $z_i = \rho_i(z)$, $i = 1, \ldots, n$. Dann ist*

$$N(z) = z_1 \cdots z_n \text{ und } \operatorname{Spur}(z) = z_1 + \cdots + z_n .$$

Beweis. Es sei zunächst $K = \mathbb{Q}[z]$ vom Grad k. Nach Lemma 7.10 ist das Minimalpolynom gleich dem charakteristischen Polynom und nach Lemma 7.13 ist das Minimalpolynom gleich $(X - z_1)(X - z_2) \cdots (X - z_k)$. Der Vergleich des konstanten Koeffizienten und des Koeffizienten zu X^{k-1} ergibt die Behauptung.

Im Allgemeinen sei

$$\mathbb{Q} \subseteq K = \mathbb{Q}[z] \subseteq L$$

und es sei M die Matrix über $\mathbb{Q}$, die die Multiplikation mit z auf K bezüglich einer $\mathbb{Q}$-Basis $y_1, \ldots, y_k$ beschreibt. Zu einer K-Basis $z_1, \ldots, z_\ell$ von L ist $y_i z_j$ eine $\mathbb{Q}$-Basis von L, und die Multiplikation mit z auf L wird durch die Blockmatrix

$$\begin{pmatrix} M & 0 & \ldots & 0 \\ 0 & M & \ldots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & M \end{pmatrix}$$

beschrieben. Deren Spur ist das ℓ-Fache der Spur von M und deren Determinante ist die ℓ-te Potenz der Determinante von M. Ebenso treten die verschiedenen komplexen Zahlen z_i jeweils ℓ-fach auf. □

Die verschiedenen Einbettungen für endliche Körpererweiterungen von $\mathbb{Q}$ führen auch zur Gittertheorie für Zahlbereiche, die wir ab der 25. Vorlesung behandeln.

Abbildungsverzeichnis