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

Zahlentheorie

Vorlesung 15

Bevor wir uns mit algebraischer Zahlentheorie, insbesondere mit quadratischen Zahlbereichen, genauer beschäftigen können, brauchen wir einige neue algebraische Begriffe. Zur Motivation betrachten wir das folgende kommutative Diagramm.

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}[i] \\ \downarrow & & \downarrow \\ \mathbb{Q} & \longrightarrow & \mathbb{Q}[i] \end{array}$$

In der unteren Zeile stehen Körper, und zwar ist $\mathbb{Q} \subset \mathbb{Q}[i]$ eine endliche Körpererweiterung vom Grad 2 (d.h. die $\mathbb{Q}$-Vektorraumdimension von $\mathbb{Q}[i]$ ist 2). Ferner ist $\mathbb{Q}$ der kleinste Körper, der die ganzen Zahlen $\mathbb{Z}$ enthält, und ebenso ist $\mathbb{Q}[i]$ der kleinste Körper, der die Gaußschen Zahlen $\mathbb{Z}[i]$ enthält. Die Gaußschen Zahlen sind, in einem zu präzisierenden Sinne, die „ganzen Zahlen“ im Körper $\mathbb{Q}[i]$.

Dies ist nicht selbstverständlich. Betrachten wir stattdessen die Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}[\sqrt{-3}]$ (ebenfalls vom Grad zwei) was ist dann der Ring der ganzen Zahlen? Es liegt das Diagramm

$$\begin{array}{ccccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}[\sqrt{-3}] & \longrightarrow & \mathbb{Z}[\omega] \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{Q} & \longrightarrow & \mathbb{Q}[\sqrt{-3}] & = & \mathbb{Q}[\sqrt{-3}] \end{array}$$

vor. Hier ist $\omega = \frac{-1+\sqrt{3}i}{2}$ und $\mathbb{Z}[\omega]$ ist der Ring der Eisenstein-Zahlen, den wir in der zweiten Vorlesung kennengelernt haben. Für die beiden Ringe $\mathbb{Z}[\sqrt{-3}]$ und $\mathbb{Z}[\omega]$ ist $\mathbb{Q}[\sqrt{-3}]$ der kleinste sie enthaltende Körper. Auf den ersten Blick wirkt vermutlich $\mathbb{Z}[\sqrt{-3}]$ natürlicher. Andererseits ist der Ring der Eisenstein-Zahlen euklidisch und damit faktoriell, hat also deutlich bessere Eigenschaften, während nach Aufgabe 5.19 $\mathbb{Z}[\sqrt{-3}]$ nicht faktoriell ist.

Im Folgenden werden wir bestimmen, was für eine beliebige endliche Körpererweiterung $\mathbb{Q} \subseteq L$ der „richtige“ Ganzheitsring in L ist. Zuerst präzisieren wir, was wir eben mit den Worten umschrieben haben, dass $\mathbb{Q}$ der kleinste Körper ist, der $\mathbb{Z}$ enthält.

Der Quotientenkörper

Definition 15.1. Zu einem Integritätsbereich R ist der *Quotientenkörper* $Q(R)$ definiert als die Menge der formalen Brüche

$$Q(R) = \left\{ \frac{r}{s} | \, r, s \in R, \, s \neq 0 \right\}$$

mit natürlichen Identifizierungen und Operationen.

Mit natürlichen Identifikationen meinen wir die (Erweiterungs- bzw. Kürzungs)-Regel

$$\frac{r}{s} = \frac{tr}{ts}$$

($t \neq 0$). Für die Operationen gelten

$$\frac{r}{s} + \frac{t}{u} = \frac{ru + ts}{su}$$

(auf einen Hauptnenner bringen) und

$$\frac{r}{s} \cdot \frac{t}{u} = \frac{rt}{su}.$$

Mit diesen Operationen liegt in der Tat, wie man schnell überprüft, ein kommutativer Ring vor. Und zwar handelt es sich um einen Körper, denn für jedes Element

$$\frac{r}{s} \neq 0$$

ist $\frac{s}{r}$ das Inverse.

Der Integritätsbereich R findet sich in $Q(R)$ über die Elemente $\frac{r}{1}$ wieder. Diese natürliche Inklusion

$$R \subseteq Q(R)$$

ist ein Ringhomomorphismus. Das Element $r = \frac{r}{1}$ hat bei $r \neq 0$ das Inverse $\frac{1}{r}$. Zwischen R und $Q(R)$ gibt es keinen weiteren Körper. Ein solcher muss nämlich zu $r \neq 0$ das (eindeutig bestimmte) Inverse $\frac{1}{r}$ enthalten und dann aber auch alle Produkte $s\frac{1}{r} = \frac{s}{r}$.

Algebraische Erweiterungen

Definition 15.2. Seien R und A kommutative Ringe und sei $R \to A$ ein fixierter Ringhomomorphismus. Dann nennt man A eine *R-Algebra*.

Wenn eine R-Algebra vorliegt, so nennt man den zugehörigen Ringhomomorphismus auch den *Strukturhomomorphismus*. Das vielleicht wichtigste Beispiel einer R-Algebra ist der Polynomring $R[X]$. Ein R-Algebra-Homomorphismus von $R[X]$ in eine weitere R-Algebra B ist durch die Zuordnung $X \mapsto f$ gegeben, wobei $f \in B$ ein beliebiges fixiertes Element ist. Diese Abbildung nennt man den *Einsetzungshomomorphismus*. Er schickt ein Polynom $\sum_{i=0}^{n} r_i X^i$, $r_i \in R$, auf $\sum_{i=0}^{n} r_i f^i \in B$, wobei die r_i via dem Strukturhomomorphismus als Elemente in B aufgefasst werden.

Definition 15.3. Sei K ein Körper und A eine kommutative K-Algebra. Es sei $f \in A$ ein Element. Dann heißt f *algebraisch* über K, wenn es ein von 0 verschiedenes Polynom $P \in K[X]$ mit $P(f) = 0$ gibt.

Wenn ein Polynom $P \neq 0$ das algebraische Element $f \in A$ annulliert (also $P(f) = 0$ ist), so kann man durch den Leitkoeffizienten dividieren und erhält dann auch ein normiertes annullierendes Polynom. Über einem Körper sind also die Begriffe ganz (siehe weiter unten) und algebraisch äquivalent.

Definition 15.4. Sei K ein Körper und A eine K-Algebra. Es sei $f \in A$ ein über K algebraisches Element. Dann heißt das normierte Polynom $P \in K[X]$ mit $P(f) = 0$, welches von minimalem Grad mit dieser Eigenschaft ist, das *Minimalpolynom* von f.

Die über den rationalen Zahlen $\mathbb{Q}$ algebraischen komplexen Zahlen erhalten einen speziellen Namen.

Definition 15.5. Eine komplexe Zahl z heißt *algebraisch* oder *algebraische Zahl*, wenn sie algebraisch über den rationalen Zahlen $\mathbb{Q}$ ist. Andernfalls heißt sie *transzendent*.

Ferdinand von Lindemann (1852-1939)

Bemerkung 15.6. Eine komplexe Zahl $z \in \mathbb{C}$ ist genau dann algebraisch, wenn es ein von 0 verschiedenes Polynom P mit rationalen Koeffizienten und mit $P(z) = 0$ gibt. Durch Multiplikation mit einem Hauptnenner kann man für eine algebraische Zahl auch ein annullierendes Polynom mit ganzzahligen Koeffizienten finden (das allerdings nicht mehr normiert ist). Eine rationale Zahl q ist trivialerweise algebraisch, da sie Nullstelle des linearen rationalen Polynoms $X - q$ ist. Weiterhin sind die reellen Zahlen $\sqrt{q}$ und $q^{1/n}$ für $q \in \mathbb{Q}$ algebraisch. Dagegen sind die Zahlen e und π nicht algebraisch. Diese Aussagen sind keineswegs selbstverständlich, die Transzendenz von π wurde beispielsweise von Ferdinand von Lindemann 1882 gezeigt.

Definition 15.7. Sei L ein Körper und $K \subseteq L$ ein Unterkörper von L. Dann heißt L ein *Erweiterungskörper* (oder *Oberkörper*) von K und die Inklusion $K \subseteq L$ heißt eine *Körpererweiterung*.

Eine K-Algebra A kann man stets in natürlicher Weise als Vektorraum über dem Körper K auffassen (ist K kein Körper, so ist eine K-Algebra ein K-Modul.) Die Skalarmultiplikation wird dabei einfach über den Strukturhomomorphismus erklärt. Durch den Vektorraumbegriff hat man sofort die folgenden Begriffe zur Verfügung.

Definition 15.8. Eine Körpererweiterung $K \subseteq L$ heißt *endlich*, wenn L ein endlichdimensionaler Vektorraum über K ist.

Definition 15.9. Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann nennt man die K-(Vektorraum-)Dimension von L den *Grad* der Körpererweiterung.

Ein Element $f \in L$ einer Körpererweiterung $K \subseteq L$ definiert durch Multiplikation eine K-lineare Abbildung

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

Über diese Konstruktion werden Norm und Spur von f erklärt.

Bemerkung 15.10. Zu einer linearen Abbildung

$$\varphi \colon V \longrightarrow V$$

eines endlichdimensionalen K-Vektorraumes V in sich wird die Determinante $\det(\varphi)$ und die Spur $S(\varphi)$ wie folgt berechnet. Man wählt eine K-Basis $v_1, \ldots, v_n \in V$ und repräsentiert die lineare Abbildung bezüglich dieser Basis durch eine quadratische $n \times n$-Matrix

$$\begin{pmatrix} \lambda_{1,1} & \cdots & \lambda_{1,n} \\ \vdots & \ddots & \vdots \\ \lambda_{n,1} & \cdots & \lambda_{n,n} \end{pmatrix}$$

mit $\lambda_{ij} \in K$ und rechnet dann die Determinante aus. Es folgt aus dem Determinantenmultiplikationssatz, dass dies unabhängig von der Wahl der Basis ist. Die Spur ist durch

$$S(\varphi) = \lambda_{1,1} + \lambda_{2,2} + \cdots + \lambda_{n,n}$$

gegeben, und dies ist nach Aufgabe 15.12 ebenfalls unabhängig von der Wahl der Basis. Norm und Spur sind Elemente aus K.

Definition 15.11. Sei $K \subseteq L$ eine endliche Körpererweiterung. Zu einem Element $f \in L$ nennt man die Determinante der K-linearen Abbildung

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

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

Definition 15.12. Sei $K \subseteq L$ eine endliche Körpererweiterung. Zu einem Element $f \in L$ nennt man die Spur der K-linearen Abbildung

$$\varphi_f \colon L \longrightarrow L,\, y \longmapsto fy,$$

die *Spur* von f. Sie wird mit $S(f)$ bezeichnet.

LEMMA 15.13. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann hat die Norm*

$$N\colon\ L \longrightarrow K,\ f \longmapsto N(f),$$

folgende Eigenschaften:

(1) *Es ist $N(fg) = N(f)N(g)$.*
(2) *Für $f \in K$ ist $N(f) = f^n$, wobei n den Grad der Körpererweiterung bezeichne.*
(3) *Es ist $N(f) = 0$ genau dann, wenn $f = 0$ ist.*

Beweis. (1) Dies folgt aus dem Determinantenmultiplikationssatz.
(2) Zu einer beliebigen Basis von L wird die Multiplikation mit einen Element aus K durch die Diagonalmatrix beschrieben, bei der jeder Diagonaleintrag f ist. Die Determinante ist dann f^n.
(3) Die eine Richtung ist klar, sei also $f \neq 0$. Dann ist f eine Einheit in L und daher ist die Multiplikation mit f eine bijektive K-lineare Abbildung $L \to L$, und deren Determinante ist $\neq 0$.

□

LEMMA 15.14. *Sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n. Dann hat die Spur*

$$S\colon\ L \longrightarrow K,\ f \longmapsto S(f),$$

folgende Eigenschaften:

(1) *Die Spur ist additiv und K-linear, also $S(f+g) = S(f) + S(g)$ und $S(\lambda f) = \lambda S(f)$ für $\lambda \in K$.*
(2) *Für $f \in K$ ist $S(f) = nf$.*

Beweis. Dies folgt aus den Definitionen. □

Eine Körpererweiterung $K \subseteq L$ heißt *einfach*, wenn sie von einem Element f erzeugt wird. Das bedeutet, dass es außer L keinen Körper zwischen K und L gibt, der f enthält. Das Element f nennt man dann auch ein *primitives Element* der Körpererweiterung. Ist L endlich und einfach, so ist

$$L\ =\ K[f]\ \cong\ K[X]/(P),$$

wobei P das Minimalpolynom von f ist.

SATZ 15.15. *Sei $K \subseteq L = K[f]$ eine einfache endliche Körpererweiterung vom Grad n. Dann hat das Minimalpolynom P von f die Gestalt*

$$P\ =\ X^n - S(f)X^{n-1} + \cdots + (-1)^n N(f).$$

Beweis. Das Minimalpolynom und das charakteristische Polynom der durch f definierten K-linearen Abbildung

$$\varphi_f\colon\ L \longrightarrow L,\ y \longmapsto fy$$

haben beide den Grad n. Nach dem Satz von Cayley-Hamilton annulliert das charakteristische Polynom die lineare Abbildung und ist somit ein Vielfaches des Minimalpolynoms, so dass sie übereinstimmen. Sei bezüglich einer Basis $v_1, \ldots, v_n$ von L diese lineare Abbildung durch die Matrix $(\lambda_{ij})_{ij}$ gegeben. Dann ist das charakteristische Polynom gleich

$$\chi_f = \det \begin{pmatrix} X-\lambda_{1,1} & \cdots & -\lambda_{1,n} \\ \vdots & \ddots & \vdots \\ -\lambda_{n,1} & \cdots & X-\lambda_{n,n} \end{pmatrix} = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0.$$

Zum Koeffizienten a_{n-1} leisten (in der Leibniz-Formel zur Berechnung der Determinante) nur diejenigen Permutationen einen Beitrag, bei denen $(n-1)$-mal die Variable X vorkommt, und das ist nur bei der identischen Permutation (also der Diagonalen) der Fall. Multipliziert man die Diagonale distributiv aus, so ergibt sich $X^n - \sum_{i=1}^n \lambda_{i,i}X^{n-1} + \ldots$, so dass also $a_{n-1} = -S(f)$ gilt. Setzt man in der obigen Gleichung $X = 0$, so ergibt sich, dass a_0 die Determinante der negierten Matrix ist, woraus $a_0 = (-1)^n N(f)$ folgt. □

Definition 15.16. Sei $K \subseteq L$ eine endliche Körpererweiterung. Sie heißt *separabel*, wenn für jedes Element $x \in L$ das Minimalpolynom separabel ist, also in keinem Erweiterungskörper eine mehrfache Nullstelle besitzt.

In unserem Zusammenhang, wo wir uns für Körpererweiterungen von $\mathbb{Q}$ interessieren, also in Charakteristik 0 sind, ist eine Körpererweiterung stets separabel (siehe Aufgabe 15.26), und wir haben den folgenden *Satz vom primitiven Element* zur Verfügung.

Satz 15.17. *Sei $K \subseteq L$ eine endliche separable Körpererweiterung. Dann wird L von einem Element erzeugt, d.h. es gibt ein $f \in L$ mit*

$$L = K(f) \cong K[X]/(P)$$

mit einem irreduziblen (Minimal-)Polynom $P \in K[X]$.

Beweis. Dies ist ein wichtiges Standardresultat aus der Theorie der Körpererweiterungen.

□

Abbildungsverzeichnis