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

Algebraische Zahlentheorie

Vorlesung 8

Die Diskriminante

Das Hauptziel dieser Vorlesung ist es, die Diskriminante einzuführen und damit zu zeigen, dass Zahlbereiche stets eine $\mathbb{Z}$-Basis besitzen.

DEFINITION 8.1. Es sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $b_1, \ldots, b_n$ Elemente in L. Dann wird die *Diskriminante* von $b_1, \ldots, b_n$ durch

$$\triangle(b_1, \ldots, b_n) = \det\left(\operatorname{Spur}(b_i b_j)_{i,j}\right)$$

definiert.

Die Produkte $b_i b_j$, $1 \leq i, j \leq n$, sind dabei Elemente in L, von denen man jeweils die Spur nimmt, die in K liegt. Man erhält also eine quadratische $n \times n$-Matrix über K. Deren Determinante ist nach Definition die Diskriminante. Im folgenden werden wir vor allem an der Diskriminante von speziellen Basen interessiert sein, so dass sich die Diskriminante als Invariante eines Zahlkörpers erweist.

Bei einem Basiswechsel verhält sich die Diskriminante wie folgt.

LEMMA 8.2. *Es sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $b_1, \ldots, b_n$ und $c_1, \ldots, c_n$ K-Basen von L. Der Basiswechsel werde durch $c = Tb$ mit der Übergangsmatrix $T = (t_{ij})_{ij}$ beschrieben. Dann gilt für die Diskriminanten die Beziehung*

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

Beweis. Ausgeschrieben haben wir die Beziehungen $c_i = \sum_{j=1}^n t_{ij} b_j$. Damit gilt

$$c_i c_k = \left(\sum_{j=1}^n t_{ij} b_j\right)\left(\sum_{m=1}^n t_{km} b_m\right) = \sum_{j,m} t_{ij} t_{km} b_j b_m.$$

Wir schreiben $c_{ik} := S(c_i c_k)$ und $b_{jm} := S(b_j b_m)$. Wegen der K-Linearität der Spur gilt

$$c_{ik} = S(c_i c_k) = S\left(\sum_{j,m} t_{ij} t_{km} b_j b_m\right) = \sum_{j,m} t_{ij} t_{km} S(b_j b_m) = \sum_{j,m} t_{ij} t_{km} b_{jm}.$$

Wir schreiben diese Gleichung mit den Matrizen $C = (c_{ik})$, $B = (b_{jm})$ und $T = (t_{ij})$ als

$$C = T^{\text{transp}} B T$$

und die Behauptung folgt dann aus dem Determinantenmultiplikationssatz und Satz 17.5 (Lineare Algebra (Osnabrück 2017-2018)). □

Bei einer endlichen Körpererweiterung $K \subseteq L$ in Charakteristik null ist die Spurabbildung $L \to K$ nicht die Nullabbildung, siehe Lemma 8.8 (Körper- und Galoistheorie (Osnabrück 2018-2019)) (2). Daraus ergibt sich auch das folgende Resultat.

LEMMA 8.3. *Es sei $K \subseteq L$ eine separable endliche Körpererweiterung vom Grad n und sei $b_1, \ldots, b_n$ eine K-Basis von L. Dann ist*

$$\triangle(b_1, \ldots, b_n) \neq 0.$$

SATZ 8.4. *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. Es 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

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

Beweis. Zunächst sind wegen Korollar 7.11 die Spuren zu Elementen aus R ganzzahlig und somit sind auch die in Frage stehenden Diskriminanten ganzzahlig. Man kann also die Diskriminanten bzw. ihre Beträge untereinander der Größe nach vergleichen.

Es sei $f \in \mathfrak{a}$ ein beliebiges Element. Wir haben zu zeigen, dass sich f als eine $\mathbb{Z}$-Linearkombination $f = k_1b_1 + \cdots + k_nb_n$ 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

$$f = q_1b_1 + \cdots + q_nb_n$$

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 (echt) zwischen 0 und 1. Dann ist auch

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

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 8.2 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 8.3 nicht 0 sind, ist dies ein Widerspruch zur Minimalität der Diskriminante. □

KOROLLAR 8.5. *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 ist $\mathfrak{a}$ eine freie abelsche Gruppe vom Rang n, d.h. es gibt Elemente $b_1, \ldots, b_n \in \mathfrak{a}$ mit*

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

wobei die Koeffizienten in einer Darstellung eines Elementes aus $\mathfrak{a}$ eindeutig bestimmt sind.

Beweis. Nach Lemma 7.7 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 (ganzzahlige) Betrag der Diskriminante minimal ist. Für diese gilt nach Satz 8.4, dass sie ein $\mathbb{Z}$-Erzeugendensystem von $\mathfrak{a}$ bilden. Die lineare Unabhängigkeit über $\mathbb{Q}$ sichert die Eindeutigkeit der Koeffizienten. □

KOROLLAR 8.6. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Dann ist R eine freie abelsche Gruppe vom Rang n, d.h. es gibt Elemente $b_1, \ldots, b_n \in R$ mit*

$$R = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n$$

derart, dass die Koeffizienten in einer Darstellung eines Elementes eindeutig bestimmt sind.

Beweis. Dies folgt direkt aus Korollar 8.5, angewendet auf das Ideal $\mathfrak{a} = R$. □

Ein solches System von Erzeugern $b_1, \ldots, b_n$ nennt man auch eine *Ganzheitsbasis* von R. Insbesondere gibt es in einem Zahlbereich stets Ganzheitsbasen. Im Ring der Eisensteinzahlen ist $1, \sqrt{-3}$ keine Ganzheitsbasis, $1, \frac{-1+\sqrt{3}}{2}$ hingegen schon. Es ergibt sich ferner, dass man eine ganzzahlige Multiplikationsmatrix erhält, wenn man als Basis eine Ganzheitsbasis nimmt. Mit dieser kann man insbesondere die Spur und die Norm ausrechnen.

DEFINITION 8.7. Es sei R der Zahlbereich zur endlichen Körpererweiterung $\mathbb{Q} \subseteq L$. Dann nennt man die Diskriminante einer Ganzheitsbasis von R die *Diskriminante* von R (und die *Diskriminante* von L).

Die Diskriminante eines Zahlbereichs (oder eines Zahlkörpers) ist eine wohldefinierte ganze Zahl. Nach Definition ist die Diskriminante so gewählt, dass sie betragsmäßig minimal unter allen Diskriminanten zu $\mathbb{Z}$-Basen aus R ist. Zwei solche Diskriminanten unterscheiden sich um ein Quadrat einer Einheit aus $\mathbb{Z}$, so dass auch das Vorzeichen wohldefiniert ist. Wir bezeichnen sie mit $\triangle_L$.

Die bisherigen Ergebnisse erlauben es, die Faserringe zu $\mathbb{Z} \subseteq R$ über einem Primideal (p) zumindest anzahlmäßig zu verstehen. Es handelt sich um endliche Ringe mit p^n Elementen. Insbesondere gibt es oberhalb von (p) stets Primideale und zwar höchstens n Stück.

KOROLLAR 8.8. *Es 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 8.6 ist $R \cong \mathbb{Z}^n$ (als abelsche Gruppen), wobei die Standardbasis der Ganzheitsbasis $a_1, \ldots, a_n$ entsprechen möge. Das von m in R erzeugte Ideal besteht aus allen $\mathbb{Z}$-Linearkombinationen der $ma_1, \ldots, ma_n$ und somit entspricht das Ideal (unter dieser Identifizierung) der von $(m, 0, \ldots, 0), (0, m, 0, \ldots, 0), \ldots, (0, \ldots, 0, m)$ erzeugten Untergruppe von $\mathbb{Z}^n$. Die Restklassengruppe $R/(m)$ ist demnach gleich $(\mathbb{Z}/(m))^n$ und besitzt m^n Elemente. Aufgrund der Ganzheit ist nach Aufgabe 6.22 $mR \cap \mathbb{Z} = m\mathbb{Z}$ und aufgrund des Homomorphiesatzes hat man einen injektiven Ringhomomorphismus

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

so dass $R/(m)$ eine von 0 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 nach Aufgabe 3.16 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). □

Weitere Berechnungsmöglichkeiten

LEMMA 8.9. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und es sei $b_1, \ldots, b_n$ eine $\mathbb{Q}$-Basis von L. Es seien $\tau_j \colon L \to \mathbb{C}$ die n verschiedenen Einbettungen in $\mathbb{C}$. Dann ist*

$$\triangle(b_1, \ldots, b_n) = (\det(\tau_j(b_k)))^2.$$

Beweis. Nach Lemma 7.14 ist die Spur eines Elementes $z \in L$ gleich der Summe $\sum_{j=1}^n \tau_j(z)$. Für ein Produkt wz ist somit

$$\text{Spur}(wz) = \sum_{j=1}^n \tau_j(wz) = \sum_{j=1}^n \tau_j(w)\tau_j(z).$$

Insbesondere ist

$$\operatorname{Spur}(b_ib_k) = \sum_{j=1}^{n} \tau_j(b_i)\tau_j(b_k).$$

Somit ist

$$(\operatorname{Spur}(b_ib_k))_{1\leq i,k\leq n} = (\tau_j(b_i))^{\mathrm{tr}}(\tau_j(b_k))$$

und daher nach Satz 17.4 (Lineare Algebra (Osnabrück 2017-2018))

$$\begin{aligned}\triangle(b_1,\ldots,b_n) &= \det(\operatorname{Spur}(b_ib_k)) \\ &= (\det(\tau_j(b_i)))^2.\end{aligned}$$

□

Besonders wichtig ist der Fall, wenn die Basis eine Basis eines Ideals oder eine Ganzheitsbasis ist. In dieser Situation fixieren wir die folgende Sprechweise.

Definition 8.10. Es sei R ein Zahlbereich vom Grad n und

$$\tau\colon R \longrightarrow \mathbb{C}^n$$

die komplexe Gesamteinbettung. Es sei $b_1,\ldots,b_n$ eine Ganzheitsbasis von R. Dann nennt man die komplexe $n\times n$-Matrix

$$(\tau_j(b_k))_{1\leq j,k\leq n}$$

die *komplexe Ganzheitsmatrix* (zu dieser Basis).

Lemma 8.11. *Es sei $\mathbb{Q}\subseteq L$ eine endliche Körpererweiterung vom Grad n und es sei $b\in L$ derart, dass die Potenzen $1,b,b^2,\ldots,b^{n-1}$ eine $\mathbb{Q}$-Basis von L bilden. Es seien $\tau_j\colon L\to\mathbb{C}$ die n verschiedenen Einbettungen in $\mathbb{C}$. Dann ist*

$$\triangle(1,b,b^2,\ldots,b^{n-1}) = \prod_{1\leq i<j\leq n}(\tau_i(b)-\tau_j(b))^2.$$

Beweis. Nach Lemma 8.9 ist die Diskriminante das Quadrat der Determinante der komplexen Matrix

$$\begin{pmatrix} 1 & \tau_1(b) & \tau_1(b)^2 & \ldots & \tau_1(b)^{n-1} \\ 1 & \tau_2(b) & \tau_2(b)^2 & \ldots & \tau_2(b)^{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \tau_{n-1}(b) & \tau_{n-1}(b)^2 & \ldots & \tau_{n-1}(b)^{n-1} \\ 1 & \tau_n(b) & \tau_n(b)^2 & \ldots & \tau_n(b)^{n-1} \end{pmatrix}.$$

Dies ist eine Vandermonde-Matrix und ihre Determinante ist gleich

$$\prod_{i<j}(\tau_i(b)-\tau_j(b)).$$

□

Abbildungsverzeichnis