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

Zahlentheorie

Vorlesung 16

Diskriminanten

DEFINITION 16.1. 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

$$\triangle(b_1, \ldots, b_n) = \det(S(b_i b_j)_{i,j})$$

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 16.2. *Sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $b_1, \ldots, b_n$ und $c_1, \ldots, c_n$ zwei 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 2015-2016)). □

LEMMA 16.3. *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*

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

Beweis. Wir beweisen diese Aussage nur in Charakteristik 0.

Sei angenommen, dass die Diskriminante 0 ist. Das bedeutet, dass das durch die Matrix $S(b_i b_j)_{ij}$ definierte lineare Gleichungssystem eine nicht-triviale Lösung $(\lambda_1, \ldots, \lambda_n)$ besitzt. Es ist also

$$\sum_{i=1}^{n} \lambda_i S(b_i b_j) = 0$$

für alle j. Sei $x = \sum_{i=1}^{n} \lambda_i b_i \neq 0$. Dann ist für jedes j

$$S(xb_j) = S\left(\left(\sum_{i=1}^{n} \lambda_i b_i\right) b_j\right) = S\left(\sum_{i=1}^{n} \lambda_i b_i b_j\right) = \sum_{i=1}^{n} \lambda_i S(b_i b_j) = 0.$$

Da x eine Einheit in L ist, ist auch xb_j, $j = 1, \ldots, n$, eine Basis und es folgt, dass die Spur auf dieser Basis und somit überall den Wert 0 hat. Dies ist aber bei einer separablen Erweiterung nicht möglich: In Charakteristik = folgt dies sofort aus Lemma 15.14 (2). □

Beschreibung von Spur und Norm mit Einbettungen

SATZ 16.4. *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 Satz 15.7 wird L durch ein Element erzeugt, es ist also

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

mit einen irreduziblen Polynom $F \in \mathbb{Q}[X]$ vom Grad n. Da F irreduzibel ist und da die Ableitung $F' \neq 0$ ist folgt, dass F und F' teilerfremd sind. Nach Satz 2.16 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. □

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 $\mathbb{Q}[i]$. Man hat die beiden Einbettung $\rho_1, \rho_2 : \mathbb{Q}[i] \to \mathbb{C}$, wobei die eine Abbildung i auf i und die andere i auf $-i$ 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. 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 16.5. *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 $M = \{z_1, \ldots, z_k\}$ die Menge der verschiedenen Werte $\rho_i(z)$. Dann gilt für das Minimalpolynom G von z die Gleichung

$$G = (X - z_1)(X - z_2) \cdots (X - z_k).$$

Beweis. 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 k über $\mathbb{Q}$. Gemäß Satz 16.4 gibt es k 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 $\sigma_i = \rho_i|_K : K \to \mathbb{C}$ 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 von einem Element erzeugt wird und das zugehörige Minimalpolynom über $\mathbb{C}$ zerfällt. Daher ist auch $M' \subseteq M$. □

Wir erwähnen ohne Beweis die folgende Beschreibung von Norm und Spur, die wir aber in der Vorlesung nicht intensiv verwenden werden.

Lemma 16.6. *Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $\rho_i : L \to \mathbb{C}$ die n verschiedenen komplexen Einbettungen. Es sei $z \in L$ und $z_i = \rho_i(z)$, $i = 1, \ldots, n$. Dann ist*

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

Beweis. Wir verzichten auf einen Beweis.

□

Moduln und Ideale

Für den Begriff des Ganzheitsringes in einem Erweiterungskörper $\mathbb{Q} \subseteq L$ benötigen wir den Begriff des Moduls, der den eines Vektorraums in dem Sinne verallgemeinert, dass der Skalarenbereich kein Körper mehr sein muss, sondern ein beliebiger kommutativer Ring sein darf.

Definition 16.7. Sei R ein kommutativer Ring und $M = (M, +, 0)$ eine *additiv* geschriebene kommutative Gruppe. Man nennt M einen *R-Modul*, wenn eine Operation

$$R \times M \longrightarrow M,\ (r, v) \longmapsto rv = r \cdot v,$$

(*Skalarmultiplikation* genannt) festgelegt ist, die folgende Axiome erfüllt (dabei seien $r, s \in R$ und $u, v \in M$ beliebig):

(1) $r(su) = (rs)u$,
(2) $r(u + v) = (ru) + (rv)$,
(3) $(r + s)u = (ru) + (su)$,
(4) $1u = u$.

Definition 16.8. Sei R ein kommutativer Ring und M ein R-Modul. Eine Teilmenge $U \subseteq M$ heißt *R-Untermodul*, wenn sie eine Untergruppe von $(M, 0, +)$ ist und wenn für jedes $u \in U$ und $r \in R$ auch $ru \in U$ ist.

Definition 16.9. Sei R ein kommutativer Ring und M ein R-Modul. Eine Familie $v_i \in M$, $i \in I$, heißt *Erzeugendensystem* für M, wenn es für jedes Element $v \in M$ eine Darstellung

$$v = \sum_{i \in J} r_i v_i$$

gibt, wobei $J \subseteq I$ endlich ist und $r_i \in R$.

Definition 16.10. Sei R ein kommutativer Ring und M ein R-Modul. Der Modul M heißt *endlich erzeugt* oder *endlich*, wenn es ein endliches Erzeugendensystem v_i, $i \in I$, für ihn gibt (also mit einer endlichen Indexmenge).

Ein kommutativer Ring R selbst ist in natürlicher Weise ein R-Modul, wenn man die Ringmultiplikation als Skalarmultiplikation interpretiert. Die Ideale sind dann genau die R-Untermoduln von R. Die Begriffe Ideal-Erzeugendensystem und Modul-Erzeugendensystem stimmen für Ideale überein.

Unter den Idealen sind besonders die Primideale und die maximalen Ideale relevant.

DEFINITION 16.11. Ein Ideal $\mathfrak{p}$ in einem kommutativen Ring R heißt *Primideal*, wenn $\mathfrak{p} \neq R$ ist und wenn für $r, s \in R$ mit $r \cdot s \in \mathfrak{p}$ folgt: $r \in \mathfrak{p}$ oder $s \in \mathfrak{p}$.

LEMMA 16.12. *Sei R ein Integritätsbereich und $p \in R$, $p \neq 0$. Dann ist p genau dann ein Primelement, wenn das von p erzeugte Hauptideal (p) ein Primideal ist.*

Beweis. Das ist trivial. □

LEMMA 16.13. *Sei R ein kommutativer Ring und $\mathfrak{p}$ ein Ideal in R. Dann ist $\mathfrak{p}$ ein Primideal genau dann, wenn der Restklassenring $R/\mathfrak{p}$ ein Integritätsbereich ist.*

Beweis. Sei zunächst $\mathfrak{p}$ ein Primideal. Dann ist insbesondere $\mathfrak{p} \subset R$und somit ist der Restklassenring $R/\mathfrak{p}$ nicht der Nullring. Sei $fg = 0$ in $R/\mathfrak{p}$ wobei f, g durch Elemente in R repräsentiert seien. Dann ist $fg \in \mathfrak{p}$ und damit $f \in \mathfrak{p}$ oder $g \in \mathfrak{p}$, was in $R/\mathfrak{p}$ gerade $f = 0$ oder $g = 0$ bedeutet.

Ist umgekehrt $R/\mathfrak{p}$ ein Integritätsbereich, so handelt es sich nicht um den Nullring und daher ist $\mathfrak{p} \neq R$. Sei $f, g \notin \mathfrak{p}$. Dann ist $f, g \neq 0$ in $R/\mathfrak{p}$ und daher $fg \neq 0$ in $R/\mathfrak{p}$, also ist $fg \notin \mathfrak{p}$. □

DEFINITION 16.14. Ein Ideal $\mathfrak{m}$ in einem kommutativen Ring R heißt *maximales Ideal*, wenn $\mathfrak{m} \neq R$ ist und wenn es zwischen $\mathfrak{m}$ und R keine weiteren Ideale gibt.

LEMMA 16.15. *Sei R ein kommutativer Ring und $\mathfrak{m}$ ein Ideal in R. Dann ist $\mathfrak{m}$ ein maximales Ideal genau dann, wenn der Restklassenring $R/\mathfrak{m}$ ein Körper ist.*

Beweis. Nach Aufgabe 9.15 entsprechen die Ideale im Restklassenring $R/\mathfrak{m}$ eindeutig den Idealen in R zwischen $\mathfrak{m}$ und R. Nun ist $R/\mathfrak{m}$ ein Körper genau dann, wenn es genau nur zwei Ideale gibt, und dies ist genau dann der Fall, wenn $\mathfrak{m} \neq R$ ist und es dazwischen kein weiteres Ideal gibt. Dies bedeutet, dass $\mathfrak{m}$ maximal ist. □

KOROLLAR 16.16. *Sei R ein kommutativer Ring und $\mathfrak{m}$ ein maximales Ideal in R. Dann ist $\mathfrak{m}$ ein Primideal.*

Beweis. Dies folgt sofort aus den Charakterisierungen für Primideale und für maximale Ideale mit den Restklassenringen. □