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

Zahlentheorie

Vorlesung 19

Wir haben zuletzt gesehen, dass ein Zahlbereich, d.h. der Ring der ganzen Zahlen in einer endlichen Körpererweiterung L von $\mathbb{Q}$, stets ein sogenannter Dedekindbereich ist. Darüber hinaus gilt auch die folgende Aussage.

Satz 19.1. *Hauptidealbereiche sind Dedekindbereiche.*

Beweis. Die Normalität folgt aus Satz 3.7 und Satz 17.12. Die Eigenschaft noethersch folgt, da in einem Hauptidealbereich jedes Ideal sogar von einem Element erzeugt wird. Die Maximalität der von 0 verschiedenen Primideale folgt aus Satz 3.12. □

Definition 19.2. 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 wollen uns im weiteren Verlauf der Vorlesung mit Ringerweiterungen $\mathbb{Z} \subseteq R$, wo R der Ring der ganzen Zahlen in einem Erweiterungskörper von $\mathbb{Q}$ ist, beschäftigen, insbesondere mit quadratischen Erweiterungen. Was bei einer solchen Erweiterung mit einer (gewöhnlichen) Primzahl p passiert, also ob sie in R ein Primelement bleibt oder nicht und welche Primideale aus $\mathfrak{p}$ über p liegen, kann man weitgehend „modulo“ p bestimmen.

Ist z. B. R durch ein in $\mathbb{Z}[X]$ irreduzibles Polynom F gegeben, also $R = \mathbb{Z}[X]/(F)$, so wird die „Faser“ (diese Terminologie lässt sich genauer begründen) über p durch den Restklassenring $(\mathbb{Z}/(p))[X]/(\overline{F})$ beschrieben (den wir auch den *Faserring* über p nennen), wobei $\overline{F}$ bedeutet, dass man jeden Koeffizient von F (der ja eine ganze Zahl ist) durch seine Restklasse in $\mathbb{Z}/(p)$ ersetzt. Dabei kann natürlich die Irreduzibilität des Polynoms verloren gehen, und dies beschreibt wichtige Eigenschaften von p in R. Man beachte hierbei die Isomorphie

$$R/pR \cong (\mathbb{Z}/(p))[X]/(\overline{F}),$$

die auf allgemeinen Gesetzen für Ideale beruht. Sie besagt insbesondere, dass p ein Primelement in R genau dann ist, wenn $\overline{F}$ irreduzibel in $(\mathbb{Z}/(p))[X]$ ist.

Insgesamt liegt eine endliche Erweiterung

$$\mathbb{Z}/(p) \subseteq (\mathbb{Z}/(p))[X]/(\overline{F})$$

vor. Dabei sind beide Ringe endlich (besitzen also nur endlich viele Elemente), und links steht ein endlicher Körper, so dass die Erweiterung also sofort ein Vektorraum ist (der selbst ein Körper sein kann, aber nicht muss) und eine gewisse Dimension besitzt (nämlich den Grad von $\overline{F}$). In diesem Abschnitt beschäftigen wir uns allgemein mit endlichen Ringen und vor allem mit endlichen Körpern.

Endliche Körper

Wir erinnern kurz an die Charakteristik eines Ringes. Zu jedem kommutativen Ring gibt es den kanonischen Ringhomomorphismus $\varphi\colon \mathbb{Z} \to \mathbb{R}$, und der Kern davon ist ein Ideal $\mathfrak{a}$ in $\mathbb{Z}$ und hat daher die Form $\mathfrak{a} = (n)$ mit einem eindeutig bestimmten $n \geq 0$. Diese Zahl nennt man die *Charakteristik* von R. Ist R ein Körper, so ist dieser Kern ein Primideal, also $\mathfrak{a} = 0$ oder $\mathfrak{a} = (p)$ mit einer Primzahl p. Man spricht von Charakteristik 0 oder von positiver Charakteristik $p > 0$. Jeder Körper umfasst einen kleinsten Körper, das ist der Körper der rationalen Zahlen $\mathbb{Q}$ bei Charakteristik 0 oder $\mathbb{Z}/(p)$ bei Charakterisitk p.

Wir erinnern ferner an den Begriff des Frobenius-Homomorphismus (siehe Aufgabe 4.12): Für einen Ring R der Charakteristik p (p eine Primzahl) ist die Abbildung $R \to R$, $f \mapsto f^p$, ein Ringhomomorphismus.

Wir haben bereits die endlichen Primkörper $\mathbb{Z}/(p)$ zu einer Primzahl p kennengelernt. Sie besitzen p Elemente, und ein Körper besitzt genau dann die Charakteristik p, wenn er diesen Primkörper enthält.

Lemma 19.3. *Sei K ein endlicher Körper. Dann besitzt K genau p^n Elemente, wobei p eine Primzahl ist und $n \geq 1$.*

Beweis. Der endliche Körper kann nicht die Charakteristik 0 besitzen, und als Charakteristik eines Körpers kommt ansonsten nach der Vorüberlegung nur eine Primzahl in Frage. Diese sei mit p bezeichnet. Das bedeutet, dass K den Körper $\mathbb{Z}/(p)$ enthält. Damit ist aber K ein Vektorraum über $\mathbb{Z}/(p)$, und zwar, da K endlich ist, von endlicher Dimension. Sei n die Dimension, $n \geq 1$. Dann hat man eine $\mathbb{Z}/(p)$-Vektorraum-Isomorphie $K \cong (\mathbb{Z}/(p))^n$ und somit besitzt K gerade p^n Elemente. □

Die vorstehende Aussage gilt allgemeiner für endliche Ringe, die einen Körper enthalten.

Endliche Körper der Anzahl p^n konstruiert man, indem man in $(\mathbb{Z}/(p))[X]$ ein irreduzibles Polynom vom Grad n findet. Ob ein gegebenes Polynom irreduzibel ist lässt sich dabei grundsätzlich in endlich vielen Schritten entscheiden, da es ja zu jedem kleineren Grad überhaupt nur endlich viele Polynome gibt,

die als Teiler in Frage kommen können. Zur Konstruktion von einigen kleinen endlichen Körpern siehe die Aufgabe 19.7.

LEMMA 19.4. *Sei K ein Körper der Charakteristik p, sei $q = p^e$, $e \geq 1$. Es sei*

$$M = \{x \in K | \, x^q = x\}.$$

Dann ist M ein Unterkörper von K.

Beweis. Zunächst gilt für jedes Element $x \in \mathbb{Z}/(p) \subseteq K$, dass

$$x^{p^e} = (x^p)^{p^{e-1}} = x^{p^{e-1}} = \ldots = x$$

ist, wobei wir wiederholt den kleinen Fermat benutzt haben. Insbesondere ist also $0, 1, -1 \in M$. Es ist $z^q = F^e(z)$ und der Frobenius

$$F\colon K \longrightarrow K, \, x \longmapsto x^p,$$

ist ein Ringhomomorphismus. Daher ist für $x, y \in M$ einerseits

$$(x+y)^q = F^e(x+y) = F^e(x) + F^e(y) = x^q + y^q = x + y$$

und andererseits

$$(xy)^q = x^q y^q = xy.$$

Ferner gilt für $x \in M$, $x \neq 0$, die Gleichheit

$$\left(x^{-1}\right)^q = (x^q)^{-1} = x^{-1},$$

so dass auch das Inverse zu M gehört und in der Tat ein Körper vorliegt. □

LEMMA 19.5. *Sei K ein Körper der Charakteristik $p > 0$, sei $q = p^e$, $e \geq 1$. Das Polynom $X^q - X$ zerfalle über K in Linearfaktoren. Dann ist*

$$M = \{x \in K | \, x^q = x\}$$

ein Unterkörper von K mit q Elementen.

Beweis. Nach Lemma 19.4 ist M ein Unterkörper von K, und nach Satz 5.1 besitzt er höchstens q Elemente. Es ist also zu zeigen, dass $F = X^q - X$ keine mehrfache Nullstellen hat. Dies folgt aber aus der formalen Ableitung $F' = -1$ und Aufgabe 19.6. □

Wenn es also einen Erweiterungskörper

$$\mathbb{Z}/(p) \subseteq K$$

gibt, über den das Polynom $X^q - X$ in Linearfaktoren zerfällt, so hat man bereits einen Körper mit q Elementen gefunden. Es gibt aber generell zu jedem Körper und jedem Polynom einen Erweiterungskörper, über dem das Polynom in Linearfaktoren zerfällt.

LEMMA 19.6. *Sei K ein Körper und F ein Polynom aus $K[X]$. Dann gibt es einen Erweiterungskörper $K \subseteq L$ derart, dass F über L in Linearfaktoren zerfällt.*

Beweis. Sei $F = P_1 \cdots P_r$ die Zerlegung in Primpolynome in $K[X]$, und sei P_1 nicht linear. Dann ist

$$K \longrightarrow K[Y]/(P_1(Y)) =: K'$$

eine Körpererweiterung von K nach Satz 3.12. Wegen $P_1(Y) = 0$ in K' ist die Restklasse y von Y in K' eine Nullstelle von P_1. Daher gilt in $K'[X]$ die Faktorisierung

$$P_1 = (X - y)\tilde{P}\,,$$

wobei $\tilde{P}$ einen kleineren Grad als P_1 hat. Das Polynom F hat also über K' mindestens einen Linearfaktor mehr als über K. Induktive Anwendung von dieser Konstruktion liefert eine Kette von Erweiterungen $K \subset K' \subset K'' \ldots$, die stationär wird, sobald F in Linearfaktoren zerfällt. □

Satz 19.7. *Sei p eine Primzahl und $e \in \mathbb{N}_+$. Dann gibt es bis auf Isomorphie genau einen Körper mit $q = p^e$ Elementen.*

Beweis. Existenz. Wir wenden Lemma 19.6 auf den Grundkörper $\mathbb{Z}/(p)$ und das Polynom $X^q - X$ an und erhalten einen Körper L der Charakteristik p, über dem $X^q - X$ in Linearfaktoren zerfällt. Nach Lemma 19.5 gibt es dann einen Unterkörper M von L, der aus genau q Elementen besteht.

Eindeutigkeit. Seien K und L zwei Körper mit q Elementen. Es sei $x \in K^\times$ ein primitives Element, das nach Satz 5.2 existiert. Daher ist $K \cong \mathbb{Z}/(p)[X]/(F)$, wobei $F \in \mathbb{Z}/(p)[X]$ das Minimalpolynom von $x \in K$ ist. Da $K^\times$ die Ordnung $q - 1$ besitzt, gilt für jede Einheit $z^{q-1} = 1$ und damit überhaupt $z^q = z$ für alle $z \in K$. D.h., dass jedes Element von K eine Nullstelle von $X^q - X$ ist und dass daher $X^q - X$ über K in Linearfaktoren zerfällt. Da insbesondere $x^q - x = 0$ ist, muss das Minimalpolynom F ein Teiler von $X^q - X$ sein, also $X^q - X = F \cdot G$. Nun zerfällt (aus den gleichen Gründen) das Polynom $X^q - X$ auch über L und insbesondere hat F eine Nullstelle $\lambda \in L$. Der Einsetzungshomomorphismus liefert einen Ringhomomorphismus

$$K \cong \mathbb{Z}/(p)[X]/(F) \longrightarrow L.$$

Da beides Körper sind, muss dieser injektiv sein. Da links und rechts jeweils q-elementige Mengen stehen, muss er auch surjektiv sein. □

Notation 19.8. Sei p eine Primzahl und $e \in \mathbb{N}_+$. Der aufgrund von Satz 19.7 bis auf Isomorphie eindeutig bestimmte endliche Körper mit $q = p^e$ Elementen wird mit

$$\mathbb{F}_q$$

bezeichnet.

Quadratische Ringerweiterungen über einem Körper

Die quadratischen Erweiterungen eines Körpers kann man wie folgt charakterisieren.

LEMMA 19.9. *Sei K ein Körper und $K \subset L$ eine Ringerweiterung vom Grad zwei. Dann gibt es die folgenden drei Möglichkeiten:*

(1) *L ist ein Körper.*
(2) *L ist von der Form $L = K[\epsilon]/\epsilon^2$.*
(3) *L ist der Produktring $L \cong K \times K$.*

Beweis. Nach Voraussetzung ist L ein zweidimensionaler K-Vektorraum. Wir können das Element $1 \in K \subset L$ zu einer K-Basis $1, u$ von L ergänzen (mit $u \notin K$). Wegen $u^2 \in L$ hat man eine Darstellung

$$u^2 = au + b$$

mit eindeutig bestimmten Elementen $a, b \in K$. Damit ist L isomorph zum Restklassenring $L \cong K[U]/(U^2 - aU - b)$. Ist das Polynom $P = U^2 - aU - b$ irreduzibel über K, so ist L ein Körper und wir sind im ersten Fall. Andernfalls gibt es eine Zerlegung $P = (U - c)(U - d)$ mit $c, d \in K$. Bei $c = d$ kann man die Restklasse von $U - c$ (also $u - c$) als ϵ bezeichnen und man ist im zweiten Fall, da ja $\epsilon^2 = 0$ gilt. Sei also $c \neq d$ vorausgesetzt. Dann induzieren die beiden K-Algebrahomomorphismen $\varphi_1 \colon L \to K$, $u \mapsto c$, und $\varphi_2 \colon L \to K$, $u \mapsto d$, einen Homomorphismus

$$\varphi = \varphi_1 \times \varphi_2 \colon L \longrightarrow K \times K.$$

Dieser ist surjektiv, da $\varphi(1) = (1, 1)$ und $\varphi(u) = (c, d)$ ist und diese Bildvektoren linear unabhängig über K sind, also eine Basis von $K \times K$ bilden. Damit ist φ aber auch injektiv und es liegt eine Isomorphie wie im dritten Fall behauptet vor. □