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

Algebraische Zahlentheorie

Vorlesung 18

Verzweigungsverhalten

Schon mehrfach hatten wir das Wort „Verzweigung“ fallen lassen. Jetzt werden wir diesen Begriff verschiedene Präzisierungen und Charakterisierungen angeben.

DEFINITION 18.1. Zu einem injektiven Ringhomomorphismus $R \subseteq S$ zwischen diskreten Bewertungsringen nennt man die Ordnung einer Ortsuniformisierenden von R in S die *Verzweigungsordnung* der Erweiterung.

Statt Verzweigungsordnung sagt man auch *Verzweigungsindex*. Bei einer Erweiterung von Dedekindbereichen

$$\varphi\colon\ R \longrightarrow S$$

und Primidealen $\mathfrak{q}$ über $\mathfrak{p}$ nennt man die Verzweigungsordnung von

$$R_{\mathfrak{p}} \longrightarrow S_{\mathfrak{q}}$$

auch die Verzweigungsordnung von $\mathfrak{q}$ über $\mathfrak{p}$ oder einfach von $\mathfrak{q}$, da ja $\mathfrak{p}$ durch $\mathfrak{q}$ bestimmt ist. Wenn man von $\mathfrak{p}$ ausgeht, hängt im Allgemeinen die Verzweigungsordnung von den darüber liegenden Primidealen ab.

DEFINITION 18.2. Ein injektiver Ringhomomorphismus $R \subseteq S$ zwischen diskreten Bewertungsringen heißt *verzweigt*, wenn seine Verzweigungsordnung ≥ 2 ist.

Bei einer Erweiterung von Dedekindbereichen $\varphi\colon\ R \to S$ sagt man auch, dass ein Primideal $\mathfrak{q}$ aus S verzweigt, wenn

$$R_{\mathfrak{p}} \longrightarrow S_{\mathfrak{q}}$$

mit $\mathfrak{p} = R \cap \mathfrak{q}$ verzweigt, und man sagt, dass ein Primideal $\mathfrak{p}$ von R in S verzweigt, wenn es darüber ein Primideal $\mathfrak{q}$ gibt, in dem Verzweigung stattfindet (es darf also auch noch Primideale darüber geben, in denen keine Verzweigung stattfindet).

LEMMA 18.3. *Es sei $R \subseteq S$ eine endliche Erweiterung von Zahlbereichen und es sei $\mathfrak{p}$ ein Primideal von R. Es sei*

$$\mathfrak{p}S = \mathfrak{q}_1^{r_1} \cdots \mathfrak{q}_k^{r_k}$$

die Idealzerlegung des Erweiterungsideales $\mathfrak{p}S$ im Sinne von Korollar 12.3. Dann ist r_j die Verzweigungsordnung von

$$R_{\mathfrak{p}} \longrightarrow S_{\mathfrak{q}_j}.$$

Insbesondere findet über $\mathfrak{p}$ genau dann Verzweigung statt, wenn ein $r_j \geq 2$ ist.

Beweis. Dies beruht darauf, dass $\mathfrak{p}$ in $S_{\mathfrak{q}_j}$ die Ordnung r_j besitzt, was auf Lemma 11.11 (1) beruht. □

Beispiel 18.4. Es sei K ein algebraisch abgeschlossener Körper. Wir betrachten den Ringhomomorphismus

$$\varphi\colon\ K[Y] \longrightarrow K[X],\ Y \longmapsto X^n,$$

zu $n \geq 2$, der der Abbildung

$$K \longrightarrow K,\ x \longmapsto x^n = y$$

entspricht. Zu einem maximalen Ideal $(X-a)$ ist

$$\varphi^{-1}(X-a) = (Y-a^n),$$

und oberhalb von $(Y-b)$ liegen die maximalen Ideale $(X-a)$ mit

$$a^n = b.$$

Dies ist die idealtheoretische Interpretation der n-ten Potenzierung. Insbesondere liegen die Ringhomomomorphismen

$$K[Y]_{(Y-b)} \longrightarrow K[X]_{(X-a)},\ Y \longmapsto X^n$$

zwischen diskreten Bewertungsringen vor. Dabei wird die Ortsuniformisierende $(Y-b)$ auf

$$X^n - b = X^n - a^n = (X-a)(X^{n-1} + X^{n-2}a^1 + \cdots + Xa^{n-2} + a^{n-1})$$

abgebildet. In dieser Produktdarstellung ist der linke Faktor die Ortsuniformisierende des zweiten Bewertungsringes. Der zweite Faktor wird, wenn man für X die Zahl a einsetzt, zu na^{n-1}. Wenn n und a beide Einheiten in K sind, so ist dieser Faktor eine Einheit in $K[X]_{(X-a)}$ und daher ist die Verzweigungsordnung gleich 1, es liegt also keine Verzweigung vor. Wenn hingegen n keine Einheit ist, wenn also die Charakteristik von K ein Teiler von n ist, so liegt Verzweigung vor. Wenn $n = p$ die positive Charakteristik ist, so ist $X^p - a^p$ und die Verzweigungsordnung ist in jedem Punkt gleich p. Wenn $a = 0$ ist, so ist die Verzweigungsordnung direkt gleich n im Nullpunkt.

Verzweigung und Ableitung

Lemma 18.5. *Es seien R, S Dedekindbereiche und es sei*

$$R \subseteq S = R[X]/(F)$$

eine monogene endliche Ringerweiterung. Es Dann ist ein Primideal $\mathfrak{p}$ von R mit perfektem Restekörper in S genau dann unverzweigt, wenn F und F' in $\kappa(\mathfrak{p})[X]$ teilerfremd sind.

Beweis. Es sei $\mathfrak{p}$ ein maximales Ideal von R und

$$\mathfrak{p}S = \mathfrak{q}_1^{r_1} \cdots \mathfrak{q}_k^{r_k}$$

die Zerlegung des Erweiterungsideales $\mathfrak{p}S$ in Ideale, die es nach Satz 12.2 gibt. Das bedeutet insbesondere, dass die Ortsuniformisierende p zu $\mathfrak{p}$ in $S_{\mathfrak{q}_j}$ die Ordnung r_j besitzt. Es liegt nach Lemma 18.3 genau dann Verzweigung vor, wenn $r_j \geq 2$ für mindestens ein j gilt. Der Faserring ist unter Verwendung von Satz 12.8 gleich

$$\kappa(\mathfrak{p})[X]/(F) = S/\mathfrak{p}S = S/\mathfrak{q}_1^{r_1} \cdots \mathfrak{q}_k^{r_k} = S/\mathfrak{q}_1^{r_1} \times \cdots \times S/\mathfrak{q}_k^{r_k}.$$

Dieser Ring ist genau dann reduziert, wenn $r_j = 1$ für alle j gilt. Deshalb folgt die Aussage aus Lemma Anhang 8.3. □

Beispiel 18.6. Es sei D eine quadratfreie Zahl $\neq 0, 1$ mit

$$D = 2, 3 \mod 4$$

und A_D der zugehörige quadratische Zahlbereich, der nach Satz 9.8 die Restklassenbeschreibung $A_D = \mathbb{Z}[X]/(X^2 - D)$ besitzt. Die Ableitung von

$$F = X^2 - D$$

ist $2X$ und somit ist, um das Verzweigungsverhalten zu verstehen, nach Lemma 18.5 das Ideal $(2X, X^2 - D)$ zu betrachten. Wenn $p \neq 2$ und kein Teiler von D ist, so ist dies über $\mathbb{Z}/(p)$ das Einheitsideal und es liegt keine Verzweigung vor. Wenn p ein Teiler von D oder $p = 2$ ist, so liegt Verzweigung mit Verzweigungsordnung 2 vor.

Bei $D = 1 \mod 4$ ist nach Satz 9.8 $A_D = \mathbb{Z}[Y]/(Y^2 - Y - \frac{D-1}{4})$. Die Ableitung ist $2Y - 1$. Oberhalb von $p = 2$ findet keine Verzweigung statt. Sei also $p \neq 2$. Modulo p ist

$$\begin{aligned} (Y^2 - Y - \frac{D-1}{4}, 2Y - 1) &= (4Y^2 - 4Y - D + 1, 2Y - 1) \\ &= 1 - 2 - D + 1 \\ &= D. \end{aligned}$$

Deshalb liegt Verzweigung genau in den Primteilern von D vor.

Korollar 18.7. *Es sei K ein algebraisch abgeschlossener Körper, $P \in K[X]$ ein nichtkonstantes Polynom und*

$$K[Y] \longrightarrow K[X] \cong K[Y][X]/(Y - P(X)),\ Y \longmapsto P(X),$$

der zugehörige Einsetzungshomomorphismus. Dann ist ein Primideal $(X-a)$ genau dann verzweigt, wenn $P'(a) = 0$ ist, und über einem Primideal $(Y-b)$ liegt genau dann Verzweigung vor, wenn es ein $a \in K$ mit $P(a) = b$ und $P'(a) = 0$ gibt.

Beweis. Wir wenden Lemma 18.5 auf die endliche Erweiterung $K[Y] \subseteq K[Y][X]/(Y - P(X))$ an. Da K algebraisch abgeschlossen ist, ist K vollkommen und der Restekörper zu jedem maximalen Ideal ist gleich K. Verzweigung oberhalb von $(Y - b)$ ist also die Frage, ob $F = Y - P(X)$ und

$F' = -P'(X)$ im Restekörper teilerfremd sind. Dabei ist Y als b zu interpretieren, es geht also darum, ob $P(X) - b$ und $P'(X)$ teilerfremd sind. Dies ist genau dann der Fall, wenn diese beiden Polynome keine gemeinsame Nullstelle in K besitzen. □

Beispiel 18.8. Es sei K ein Körper der Charakteristik $p > 0$. Wir betrachten die Ringerweiterung

$$K(t)[Y] \subseteq K(t)[Y][X]/(X^p - t) = K(t)[X]/(X^p - t)[Y] \cong K(x)[Y],$$

die Erweiterung spielt sich also im Wesentlichen im Grundkörper ab. Es ist

$$(X^p - t)' = pX^{p-1} = 0,$$

deshalb sind das beschreibende Polynom und seine Ableitung nirgendwo teilerfremd. Dennoch ist

$$K(t)[Y]_{(Y)} \longrightarrow K(x)[Y]_{(Y)}$$

unverzweigt, da Y in beiden Ringen die Ortsuniformisierende ist. Dies zeigt auch, dass Lemma 18.5 ohne die Voraussetzung über die Perfektheit nicht gilt.

Satz 18.9. *Es sei R ein Dedekindbereich mit Quotientenkörper $K = Q(R)$, es sei $K \subseteq L$ eine separable Körpererweiterung und S der ganze Abschluss von R in L. Dann gibt es nur endlich viele Primideale von R, über denen Verzweigung stattfindet.*

Beweis. Es sei

$$L = K[x] = K[X]/(F)$$

mit einem normierten Polynom F, was es nach dem Satz vom primitiven Element gibt. Wir betrachten die endlichen Abbildungen

$$R \subseteq R[x] \cong R[X]/(F) \subseteq S$$

wobei S die Normalisierung von $R[x]$ ist. Es sei

$$S = R[x][\frac{g_1}{f_1}, \ldots, \frac{g_n}{f_n}]$$

mit $g_i, f_i \in R[x]$ und wobei wir $f_i \in R$ annehmen dürfen. Sei

$$f = \prod f_i \neq 0.$$

Dann ist

$$R_f[x] = R[x]_f = S_f.$$

Das heißt, dass oberhalb von R_f der Ganzheitsring durch ein Element erzeugt wird. Da es oberhalb von (f) nur endlich viele Primideale in R gibt, genügt es zu zeigen, dass in $D(f)$ nur endlich viele Primideale verzweigen. Wir können also

$$S = R[x]$$

als monogen annehmen. Wir betrachten das von F und F' erzeugte Ideal in $R[X]$. Wegen der Separabilität der generischen Körpererweiterung erzeugen

diese Polynome in $K[X]$ das Einheitsideal, was in $R[X]$ bedeutet, dass es Polynome P, Q gibt mit

$$FP + F'Q = g \in R$$

mit $g \neq 0$. Dies heißt wiederum, dass in $R_g[X]$ die beiden Polynome das Einheitsideal erzeugen. Somit findet nach Lemma 18.5 auf $D(g)$ keine Verzweigung statt. Oberhalb von g gibt es aber auch wieder nur endlich viele Primideale und die Primideale aus $D(g)$ verzweigen nicht. □

Verzweigung und Faserringe

In Lemma 15.1 und Lemma 15.7 haben wir von der Reduziertheit der Faserringe auf die Normalität des (lokalisierten) Zahlbereiches geschlossen. Wir werden sehen, dass diese Reduziertheit direkt mit der Unverzweigtheit zusammenhängt und dass diese somit stärker als die Normalität ist.

Satz 18.10. *Es sei $R \subseteq S$ eine endliche Erweiterung von Zahlbereichen und es sei $\mathfrak{p}$ ein Primideal von R. Es sei*

$$\mathfrak{p}S = \mathfrak{q}_1^{r_1} \cdots \mathfrak{q}_k^{r_k}$$

die Idealzerlegung des Erweiterungsideales $\mathfrak{p}S$ im Sinne von Korollar 12.3. Dann ist $\mathfrak{p}$ in S genau dann verzweigt, wenn der Faserring zu S über $\mathfrak{p}$ nicht reduziert ist.

Beweis. Nach Korollar 12.3 liegt in S eine Produktzerlegung

$$\mathfrak{p}S = \mathfrak{q}_1^{r_1} \cdots \mathfrak{q}_k^{r_k}$$

vor und nach Satz 12.8 ist

$$S/\mathfrak{p}S \cong S/\mathfrak{q}_1^{r_1} \times \cdots \times S/\mathfrak{q}_k^{r_k}.$$

Dieser Restklassenring, der der Faserring zu S über $\mathfrak{p}$ ist, ist genau dann reduziert, wenn alle Exponenten r_i gleich 1 sind. Dies charakterisiert nach Lemma 18.3 auch die Unverzweigtheit. □

Beispiel 18.11. Es sei p eine Primzahl und $R = \mathbb{Z}[X]/(X^p - p)$. Für eine Primzahl $q \neq p$ ist der Faserring über (q) gleich $\mathbb{Z}/(q)[X]/(X^p - p)$. Da p eine Einheit in $\mathbb{Z}/(q)$ ist, sind $X^p - p$ und die Ableitung pX^{p-1} teilerfremd in $\mathbb{Z}/(q)[X]$ und daher ist nach Korollar 15.2 $\mathbb{Z}_p[X]/(X^p - p)$ normal und die Verzweigungsordnung von

$$\mathbb{Z}_{(q)} \longrightarrow R_{\mathfrak{q}},$$

wobei $\mathfrak{q}$ ein Primideal oberhalb von (q) bezeichnet, ist gleich 1. Für $q = p$ ist das einzige Primideal oberhalb von (p) das Hauptideal (X), die Verzweigungsordnung in p ist gleich p. Deshalb ist insgesamt R der Zahlbereich zu $\mathbb{Q} \subset \mathbb{Q}[X]/(X^p - p)$, und er ist nur im Punkt (p) verzweigt.

Beispiel 18.12. Es seien p, q verschiedene Primzahlen und $R = \mathbb{Z}[X]/(X^p - q)$. Für eine Primzahl $r \neq p, q$ ist der Faserring über (r) gleich $\mathbb{Z}/(r)[X]/(X^p - q)$. Da p und q Einheiten in $\mathbb{Z}/(r)$ sind, gilt

$$\begin{aligned}(X^p - q, pX^{p-1}) &= (X^p - q, X^{p-1}) \\ &= (q, X^{p-1}) \\ &= (q) \\ &= 1\end{aligned}$$

in $\mathbb{Z}/(r)[X]$, d.h. $X^p - q$ und die Ableitung pX^{p-1} sind teilerfremd in $\mathbb{Z}/(r)[X]$ und daher ist nach Korollar 15.2 $\mathbb{Z}_r[X]/(X^p - q)$ normal und die Verzweigungsordnung von

$$\mathbb{Z}_{(r)} \longrightarrow R_{\mathfrak{r}},$$

wobei $\mathfrak{r}$ ein Primideal oberhalb von (r) bezeichnet, ist gleich 1.

Für $r = q$ ist das einzige Primideal oberhalb von (q) das Hauptideal (X), die Verzweigungsordnung in q ist gleich p.

Für $r = p$ ist der Faserring gleich

$$\mathbb{Z}/(p)[X]/(X^p - q) = \mathbb{Z}/(p)[X]/(X - q)^p.$$

Das einzige Primideal oberhalb von (p) ist also $(X - q, p)$, was im Allgemeinen kein Hauptideal ist. Der Ring R ist im Allgemeinen nicht der ganze Abschluss, wobei die Singularität oberhalb von (p) liegt.

Verzweigung und Diskriminante

Die Faserringe zu einem Zahlbereich über einer Primzahl p sind im Allgemeinen kein Körper, sie sind aber freie endlich erzeugte $\mathbb{Z}/(p)$-Algebren und daher ist dort auch die Spur und die Diskriminante (allerdings aber nur bis auf eine Einheit) definiert. Unter der *Spurform* auf einer freien K-Algebra A versteht man die symmetrische Bilinearform

$$A \times A \longrightarrow K,\ (x, y) \longmapsto \operatorname{Spur}(xy).$$

Satz 18.13. *Es sei K ein vollkommener Körper und A eine endlichdimensionale K-Algebra. Dann sind folgende Aussagen äquivalent.*

(1) *A ist reduziert.*
(2) *A ist ein Produkt von Körpern.*
(3) *Die Spurform ist nichtausgeartet.*
(4) *Die Diskriminante ist ungleich 0.*

Beweis. Die Äquivalenz von (1) und (2) ist klar aufgrund von Aufgabe 17.1. Sei (2) erfüllt, $A = L_1 \times \cdots \times L_r$. Wegen der Voraussetzung vollkommen sind die Körpererweiterungen $K \subseteq L_j$ separabel. Die Spur $A \to K$ setzt sich zusammen aus der Summe der Spuren zu den Körpererweiterungen, da man von diesen jeweils Basen wählen kann und sich diese zu einer Gesamtbasis

von A zusammensetzen. Bezüglich einer solchen Basis sind die Multiplikationsmatrizen Diagonalblockmatrizen. Bei $x \in A$ von 0 verschieden ist auch eine Komponente x_j in einem Körper L_j von 0 verschieden. Im Körperfall ist die Spurform nichtausgeartet und daher gibt es $y_j \in L_j$ (das wir in A auffassen können) mit $S(x, y_j) = S(x_j y_j) \neq 0$. (3) und (4) sind äquivalent. Wenn die Spurform nicht ausgeartet ist, so besitzt die Gramsche Matrix davon eine von 0 verschiedene Determinante, und umgekehrt, siehe Aufgabe 38.13 (Lineare Algebra (Osnabrück 2017-2018)) bzw. Lemma 8.3.

Sei nun A nicht reduziert. Zu einem nilpotenten Element f ist das Minimalpolynom gleich X^m und damit ist auch das charakteristische Polynom gleich X^n, wobei n den Grad der Erweiterung bezeichnet (für einen Körper A wurde dies in Lemma 7.10 gezeigt, es gilt aber auch sonst). Deshalb ist die Spur von f nach Aufgabe 7.17 gleich 0. Zu einem nilpotenten Element f und einem beliebigen Element x ist auch fx nilpotent und daher ist, wenn es ein nichttriviales nilpotentes Element gibt, die Spurform ausgeartet. □

Lemma 18.14. *Es sei R ein Zahlbereich, $f \in R$ und p eine Primzahl. Dann ist die Spur von f modulo p gleich der im Faserring $R/(p)$ über $\mathbb{Z}/(p)$ berechneten Spur von $\overline{f} \in R/(p)$.*

Beweis. Nach Korollar 8.6 ist R ein freier $\mathbb{Z}$-Modul, dessen Rang der Grad n der zugrunde liegenden Körpererweiterung ist, und nach Korollar 8.8 ist der Faserring über $\mathbb{Z}/(p)$ eine n-dimensionale $\mathbb{Z}/(p)$-Algebra. In beiden Fällen kann man also die Spur über die Multiplikationsmatrix bezüglich einer Basis berechnen. Sei eine $\mathbb{Z}$-Basis $b_1, \ldots, b_n$ von R fixiert. Eine $\mathbb{Z}$-Basis von R wird modulo p zu einer $\mathbb{Z}/(p)$-Basis von $R/(p)$, siehe den Beweis zu Korollar 8.8. In der Multiplikationsmatrix zu f bezüglich $b_1, \ldots, b_n$ stehen die ganzen Zahlen c_{ij}, die durch

$$fb_i = \sum_{j=1}^{n} c_{ij} b_j$$

gegeben sind. Da $R \to R/(p)$ ein Ringhomomorphismus ist, folgt

$$\overline{fb}_i = \sum_{j=1}^{n} \overline{c}_{ij} \overline{b}_j$$

und daher ist die Multiplikationsmatrix zu $\overline{f}$ bezüglich $\overline{b}_1, \ldots, \overline{b}_n$ einfach die komponentenweise reduzierte Matrix. Deshalb ist insbesondere die Reduktion der Spur

$$\operatorname{Spur}(f) = \sum_{i=1}^{n} c_{ii}$$

gleich $\sum_{i=1}^{n} \overline{c}_{ii}$, also gleich der Spur der Reduktion. □

Satz 18.15. *Es sei R ein Zahlbereich mit Diskriminante $\triangle_R$. Es sei p eine Primzahl. Dann ist p genau dann ein Teiler von $\triangle_R$, wenn der Faserring zu R über p nicht reduziert ist.*

Beweis. Es sei $b_1, \ldots, b_n$ eine Ganzheitsbasis von R. Die Matrix M mit den Einträgen Spur $(b_i b_j)$ ist die Gramsche Matrix der Spurform. Die Gramsche Matrix M' der Spurform zu $R/(p)$ über $\mathbb{Z}/(p)$ bezüglich der $\mathbb{Z}/(p)$-Basis $\overline{b}_1, \ldots, \overline{b}_n$ entsteht daraus nach Lemma 18.14 durch komponentenweise Reduktion. Da das Berechnen der Determinante mit beliebigen Ringwechseln verträglich ist, ist die Determinante von M' gleich der Determinante von M (also der Diskriminante von R) modulo p genommen. Somit ist p genau dann ein Teiler der Diskriminante von R, wenn die Diskriminante des Faserringes gleich 0 ist. Dies ist nach Satz 18.13 äquivalent dazu, dass der Faserring nicht reduziert ist. □

Abbildungsverzeichnis