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

# Algebraische Zahlentheorie

## Vorlesung 15

### Normalitätskriterien

Es ist im Allgemeinen schwierig, den ganzen Abschluss von $\mathbb{Z}$, also den Zahlbereich, in einer endlichen Körpererweiterung $\mathbb{Q} \subseteq L$ zu bestimmen bzw. eine vorliegende Ringerweiterung

$$\mathbb{Z} \subseteq S = \mathbb{Z}[X_1, \ldots, X_m]/(F_1, \ldots, F_n) \subseteq L$$

als normal nachzuweisen. Es handelt es sich aber um ein lokales Problem, d.h. $S$ ist genau dann normal, wenn $S_{\mathfrak{p}}$ für jedes Primideal $\mathfrak{p}$ normal ist, und dies ist genau dann der Fall, wenn für jede Primzahl $p$ die Nenneraufnahme $S_{\mathbb{Z}\setminus\mathbb{Z}p}$ normal ist, siehe Aufgabe 6.16 und Aufgabe 15.1. Dies erlaubt den Übergang zu einem diskreten Bewertungsring als Basisring ($\mathbb{Z}_{(p)}$ statt $\mathbb{Z}$), was oft die Gleichungsbeschreibung vereinfacht und was es erlaubt, Eigenschaften der Faserringe $S/pS$ besser zu verarbeiten. Das typische Verhalten ist, dass sich die Ringe $S_{\mathbb{Z}\setminus\mathbb{Z}p}$ bis auf endliche viele Primzahlen direkt als normal erweisen, und dass man einen Teil der verbleibenden Ringe über Eigenschaften der Faser erledigen kann, einen anderen Teil aber auch nicht.

Lemma 15.1. *Es sei $B$ ein diskreter Bewertungsring mit Ortsuniformisierender $p$ und sei $F \in B[X]$ ein normiertes irreduzibles Polynom. Sei $R = B[X]/(F)$. In der Zerlegung von $F$ in $B/(p)[X]$ in irreduzible Faktoren, $F = F_1 \cdots F_s$, seien alle Faktoren einfach. Dann ist $R$ der ganze Abschluss von $B$ in $Q(B)[X]/(F)$ und insbesondere normal.*

*Beweis.* Wir können direkt annehmen, dass die $F_i$ zu $B[X]$ gehören. Die maximalen Ideale von $R$ sind $(p, F_j)$ für $j = 1, \ldots, s$. Die Voraussetzung bedeutet für $B[X]$ die Beziehung $F_1 \cdots F_s = F + pH$ und für

$$R = B[X]/(F)$$

die Gleichheit

$$F_1 \cdots F_s = pH.$$

Da $F_i$ und $F_j$ teilerfremd sind, sind die $F_i$ Einheiten in der Lokalisierung $R_{(p,F_j)}$ und daher ist

$$F_j = \frac{H}{F_1 \cdots F_{j-1} F_{j+1} \cdots F_s} \cdot p.$$

D.h. in $R_{(p,F_j)}$ ist das maximale Ideal ein Hauptideal mit dem Erzeuger $p$ und daher liegt nach Satz 10.17 ein diskreter Bewertungsring vor. Somit ist $R$ normal. □

Die Beispielklasse $\mathbb{Z}_{(2)}[X]/(X^2-D)$, wo der Faserring immer einen mehrfachen Faktor besitzt, zeigt, dass Lemma 15.1 keine notwendige Voraussetzung für die Normalität ist. Die Bedingung, dass in der Primfaktorzerlegung von $F$ in $B/(p)[X]$ jeder Faktor einfach ist, kann man auch so formulieren, dass der Faserring

$$R/(p) \,=\, B[X]/(F,p) \,=\, B/(p)[X]/(F)$$

reduziert ist. Bei $F \,=\, F_1^{r_1} \cdots F_s^{r_s}$ in $B/(p)[X]$ gilt ja generell nach Satz 12.11 die Beziehung

$$B/(p)[X]/(F) \,=\, B/(p)[X]/(F_1^{r_1}) \times \cdots \times B/(p)[X]/(F_s^{r_s}),$$

und dies ist genau dann reduziert, wenn jeder Komponentenring reduziert ist, und dies ist genau dann der Fall, wenn jeder Komponentenring ein Körper ist, also genau bei $r_j \,=\, 1$ für alle $j$. Im Allgemeinen, wenn beispielsweise der Ring durch mehrere Variablen und Gleichungen beschrieben wird, ist die Beschreibung mit reduziert wichtiger, bei nur einer Gleichung lässt sich aber die Bedingung in Lemma 15.1 einfacher überprüfen.

Korollar 15.2. *Es sei $B$ ein diskreter Bewertungsring mit Ortsuniformisierender $p$ und sei $F \in B[X]$ ein normiertes irreduzibles Polynom. Es seien $F$ und $F'$ in $B/(p)[X]$ teilerfremd. Dann ist $R \,=\, B[X]/(F)$ normal und gleich dem ganzen Abschluss von $B$ in $Q(B)[X]/(F)$.*

*Beweis.* Dies folgt aus Lemma 15.1 in Verbindung mit einer Variante von Aufgabe 7.35. □

Korollar 15.3. *Es sei $F \in \mathbb{Z}[X]$ ein normiertes irreduzibles Polynom, $R \,=\, \mathbb{Z}[X]/(F)$. Dann ist bis auf endlich viele Primzahlen $p$ der Ring*

$$R_{\mathbb{Z}\setminus(p)} \,=\, \mathbb{Z}_{(p)}[X]/(F)$$

*normal.*

*Beweis.* Wir betrachten $F$ als irreduzibles Polynom in $\mathbb{Q}[X]$. In Charakteristik 0 sind $F$ irreduzibel und $F'$ teilerfremd. Deshalb gibt es Polynome $A,B \in \mathbb{Q}[X]$ mit $AF+BF' \,=\, 1$. Es sei $m \in \mathbb{Z}$ ein Hauptnenner der Koeffizienten von $A$ und $B$. Dann gibt es Polynome $C,D \in \mathbb{Z}[X]$ mit $CF+DF' \,=\, m$. Für jede Primzahl $p$, die kein Teiler von $m$ ist, gilt entsprechend $CF+DF' \,=\, m$ in $\mathbb{Z}/(p)[X]$ und $m$ ist dort eine Einheit. Deshalb sind $F,F'$ in $\mathbb{Z}/(p)[X]$ teilerfremd und die Normalität von $\mathbb{Z}_{(p)}[X]/(F)$ folgt aus Korollar 15.2. □

Beispiel 15.4. Wir betrachten das kubische Polynom $X^3-3X+1 \in \mathbb{Q}[X]$, das nach Aufgabe 2.25 irreduzibel ist, und $R \,=\, \mathbb{Z}[X]/(X^3-3X+1)$. Die Ableitung des Polynoms ist $3X^2-3$, und in $\mathbb{Z}[X]$ gilt die Gleichung

$$(6X+3)(X^3-3X+1)+(-2X^2-X+4)(3X^2-3) \,=\, -9.$$

Nach dem Beweis zu Korollar 15.3 ist daher $\mathbb{Z}_{(p)}[X]/(X^3-3X+1)$ für jede Primzahl $p \neq 3$ normal. Über $p = 3$ ist der Faserring gleich

$$\mathbb{Z}/(3)[X]/(X^3-3X+1) = \mathbb{Z}/(3)[X]/(X^3+1) = \mathbb{Z}/(3)[X]/(X+1)^3.$$

Dies bedeutet, dass das einzige maximale Ideal in $\mathbb{Z}_{(3)}[X]/(X^3-3X+1)$ gleich $(3, X+1)$ ist. Wegen

$$\mathbb{Z}_{(3)}[X]/(X^3-3X+1, X+1) = \mathbb{Z}_{(3)}/((-1)^3-3(-1)+1) = \mathbb{Z}/(3)$$

ist aber $X+1$ ein Erzeuger von diesem maximalen Ideal und daher ist $R$ überhaupt normal.

Lemma 15.5. *Es sei $F \in \mathbb{Z}[X]$ ein normiertes irreduzibles Polynom, $R = \mathbb{Z}[X]/(F)$ und sei $p$ eine Primzahl derart, dass in $\mathbb{Z}/(p)[X]$ die Zerlegung*

$$F = F_1^{r_1} \cdots F_s^{r_s}$$

*mit irreduziblen Polynomen $F_j$ gelte. Dann gilt in $R$ die Gleichheit*

$$pR = (p, F_1^{r_1}) \cdots (p, F_s^{r_s}).$$

*Beweis.* In $\mathbb{Z}/(p)[X]$ sind die $F_j$ zueinander paarweise teilerfremd. Wir behaupten, dass in $\mathbb{Z}[X]/(F)$ die Gleichheit

$$(p) = (p, F_1^{r_1}) \cap \ldots \cap (p, F_s^{r_s}) = (p, F_1^{r_1}) \cdots (p, F_s^{r_s})$$

gilt, wobei die letzte Gleichheit auf Lemma 12.6 beruht. Zum Nachweis der linken Gleichheit sei

$$a = a_1 p + b_1 F_1^{r_1} = \ldots = a_s p + b_s F_s^{r_s},$$

es ist $a \in (p)$ zu zeigen. Modulo $p$ ist

$$a = b_1 F_1^{r_1} = \ldots = b_s F_s^{r_s}$$

in $\mathbb{Z}/(p)[X]/(F)$. Nach Satz 12.11 ist

$$\mathbb{Z}/(p)[X]/(F) = \mathbb{Z}/(p)[X]/(F_1^{r_1}) \times \cdots \times \mathbb{Z}/(p)[X]/(F_s^{r_s}).$$

Die Voraussetzung bedeutet, dass $a$ in jeder Komponente 0 ist, also insgesamt gleich 0 ist. □

Korollar 15.6. *Es sei $F \in \mathbb{Z}[X]$ ein normiertes irreduzibles Polynom, $R = \mathbb{Z}[X]/(F)$ und sei $p$ eine Primzahl derart, dass der Faserring $\mathbb{Z}/(p)[X]/(F)$ reduziert ist. Dann ist $pR$ das Produkt von Primidealen.*

*Beweis.* Dies folgt aus Lemma 15.5, da im reduzierten Fall die Exponenten $r_j = 1$ sind, und dann $(p, F_j)$ Primideale sind, oder aus Lemma 15.1 in Verbindung mit Satz 12.2. □

Ohne die Voraussetzung reduziert ist die Aussage nicht richtig, siehe Beispiel 12.9.

Wir behandeln noch den Fall, wo die Algebra durch mehrere Variablen erzeugt wird. Dies ergibt auch einen weiteren Beweis für Lemma 15.1.

LEMMA 15.7. *Es sei $B$ ein diskreter Bewertungsring mit Ortsuniformisierender $p$ und es sei $R = B[X_1, \ldots, X_n]/\mathfrak{a}$. eine endliche integre $B$-Algebra. Der Faserring $R/pR$ sei reduziert. Dann ist $R$ normal.*

*Beweis.* Es sei $\mathfrak{p}$ ein maximales Ideal von $R$. Wir betrachten das kommutative Diagramm

$$\begin{array}{ccccc} B & \longrightarrow & R & \longrightarrow & R_{\mathfrak{p}} \\ \downarrow & & \downarrow & & \downarrow \\ B/(p) & \longrightarrow & R/pR & \longrightarrow & (R/pR)_{\mathfrak{p}} \cong R_{\mathfrak{p}}/pR_{\mathfrak{p}} \ . \end{array}$$

Als Lokalisierung eines nach Voraussetzung reduzierten Ringes ist der Ring rechts unten reduziert, also hier sogar ein Körper. Dies heißt aber, dass

$$(p)R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$$

gilt und das bedeutet, dass $R_{\mathfrak{p}}$ ein diskreter Bewertungsring ist. □

## Monogene Algebren

DEFINITION 15.8. Eine $R$-Algebra $A$ über einem kommutativen Ring $R$ heißt *monogen*, wenn sie als $A = R[X]/\mathfrak{a}$ mit einem Ideal $\mathfrak{a} \subseteq R[X]$ geschrieben werden kann.

Nach dem Satz vom primitiven Element ist eine endliche separable Körpererweiterung $K \subseteq L$ stets monogen, was man auf jede endliche Körpererweiterung $\mathbb{Q} \subseteq L$ anwenden kann. Ferner ist nach Satz 9.8 jeder quadratische Zahlbereich monogen über $\mathbb{Z}$. Ein Zahlbereich ist genau dann monogen, wenn es ein Element mit der Eigenschaft gibt, dass seine Potenzen eine Ganzheitsbasis bilden.

LEMMA 15.9. *Es sei $(B, \mathfrak{p}) \subseteq (S, \mathfrak{q})$ eine endliche Erweiterung von diskreten Bewertungsringen. Es sei $h \in S$ eine Ortsuniformisierende derart, dass*

$$\kappa(\mathfrak{p})[\overline{h}] = \kappa(\mathfrak{q})$$

*gilt. Dann ist $S = B[h]$.*

*Beweis.* Wir betrachten die endliche Erweiterung

$$R = B[h] \subseteq S,$$

die als identisch nachzuweisen ist. Es ist $\mathfrak{m} = B[h] \cap \mathfrak{q}$ das maximale Ideal von $B[h]$, der ebenfalls ein lokaler Ring ist, und es ist $\mathfrak{m}S = hS = \mathfrak{q}$. Ferner ist

$$B[h] + hS = S.$$

Für $f \in S$ gilt ja im Restekörper $\kappa(\mathfrak{q})$

$$\overline{f} = \overline{P}(\overline{h})$$

mit einem Polynom $\overline{P}$ über $\kappa(\mathfrak{p})$. In $S$ gilt deshalb

$$f \;=\; P(h) + hg$$

mit $g \in S$. Nach dem Lemma von Nakayama gilt $R = S$. □

Beispiel 15.10. Wir betrachten die biquadratische Erweiterung

$$\mathbb{Z} \subseteq \mathbb{Z}[X,Y]/(X^2-7, Y^2-19).$$

Dieser Ganzheitsring lässt sich nicht in der Form $\mathbb{Z}[W]/(F)$ schreiben. Modulo (3) ist der Faserring gleich

$$\begin{aligned} \mathbb{Z}/(3)[X,Y]/(X^2-7, Y^2-19) &= \mathbb{Z}/(3)[X,Y]/(X^2-1, Y^2-1) \\ &= \mathbb{Z}/(3) \times \mathbb{Z}/(3) \times \mathbb{Z}/(3) \times \mathbb{Z}/(3), \end{aligned}$$

er besitzt also vier maximale Ideale, alle mit dem Restekörper $\mathbb{Z}/(3)$. Ein Ring der Form $\mathbb{Z}/(3)[W]/(F)$ kann aber nur drei maximale Ideale mit dem Restekörper $\mathbb{Z}/(3)$ besitzen, da es in $\mathbb{Z}/(3)$ nur drei Elemente gibt. Es folgt, dass der Ganzheitsring auch nicht über der Lokalisierung $\mathbb{Z}_{(3)}$ mit einem einzigen Algebraerzeuger beschrieben werden kann.

# Abbildungsverzeichnis