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

Algebraische Zahlentheorie

Vorlesung 20

Zerlegungsverhalten

Wir besprechen nun systematisch, wie eine Primzahl p in einem Zahlbereich R zerlegt wird, also wie viele Primideale von R oberhalb von (p) liegen, wie diese sich zueinander verhalten und wie die Abhängigkeit von p aussieht. Viele Eigenschaften hängen dabei allein vom Faserring R/pR ab, von dem wir nach Korollar 8.8 wissen, dass R/pR als additive Gruppe isomorph zu $(\mathbb{Z}/(p))^n$ ist, wenn n der Grad der Erweiterung ist.

Definition 20.1. Es sei $R \subseteq S$ eine endliche Erweiterung von kommutativen Ringen, sei $\mathfrak{p}$ ein Primideal von R und $\mathfrak{q}$ ein Primideal von S über $\mathfrak{p}$. Dann nennt man den Grad der Erweiterung der Restekörper $\kappa(\mathfrak{p}) \subseteq \kappa(\mathfrak{q})$ den *Trägheitsgrad* von $\mathfrak{q}$ über $\mathfrak{p}$.

Bemerkung 20.2. Wenn $R \subseteq S$ eine endliche Erweiterung von Dedekindbereichen ist und $\mathfrak{m}$ ein maximales Ideal von R ist und $\mathfrak{n}$ ein maximales Ideal von S über $\mathfrak{m}$, so ist der Trägheitsgrad einfach der Grad der Körpererweiterung

$$R/\mathfrak{m} \longrightarrow S/\mathfrak{n}$$

(der Trägheitsgrad im Nullideal ist einfach der Grad der Erweiterung der Quotientenkörper). Wenn R und damit auch S ein Zahlbereich ist, so sind diese Körper stets endlich von gleicher Charakteristik p, und daher liegt eine Erweiterung der Form $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ mit $q = p^e$ und $q' = p^{e'}$ vor.

Lemma 20.3. *Es sei R ein kommutativer Ring und $R \subseteq S$ eine endliche Erweiterung der Form $S = R[X]/(F)$ mit einem normierten Polynom $F \in R[X]$ vom Grad d. Es sei $\mathfrak{p}$ ein Primideal von R. Dann ist die Summe über alle Trägheitsgrade zu Primidealen über $\mathfrak{p}$ durch d beschränkt.*

Beweis. Durch Übergang mittels $R \to \kappa(\mathfrak{p})$ kann man direkt annehmen, dass $R = K$ ein Körper ist und dass das Primideal das Nullideal ist. Es liegt dann die endliche Erweiterung $K \subseteq K[X]/(F) =: B$ vor. Die Primideale von S oberhalb von $\mathfrak{p}$ entsprechen den Primidealen von B und damit den irreduziblen Teilern von F in $K[X]$. Sei $F = F_1^{n_1} \cdots F_k^{n_k}$ die Primfaktorzerlegung von F in $K[X]$. Die relevanten Körpererweiterungen sind dann die

$$K \subseteq K[X]/(F_j).$$

Die Aussage folgt daher direkt aus Gradeigenschaften von Polynomen über einem Körper. $\square$

Satz 20.4. *Es sei R ein Dedekindbereich mit Quotientenkörper K, $K \subseteq L$ eine Körpererweiterung vom Grad n und S der ganze Abschluss von R in L. Es sei $\mathfrak{p}$ ein von 0 verschiedenes Primideal von R mit der Primidealzerlegung*

$$\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_k^{e_k}$$

in S. Die Körpererweiterungen $\kappa(\mathfrak{p}) \subseteq \kappa(\mathfrak{q}_j)$ haben die Trägheitsgrade f_j. Dann ist

$$n = \sum_{j=1}^{k} e_j f_j.$$

Beweis. Nach dem chinesischen Restsatz für Dedekindbereiche ist

$$S/\mathfrak{p}S = S/\mathfrak{q}_1^{e_1} \times \cdots \times S/\mathfrak{q}_k^{e_k}.$$

Wir können über dem diskreten Bewertungsring $R_{\mathfrak{p}}$ argumentieren, also davon ausgehen, dass R ein diskreter Bewertungsring mit dem maximalen Ideal $\mathfrak{p}$ ist. Die angeführten Restklassenringe ändern sich dadurch nicht. Es ist S ein freier R-Modul vom Rang n und somit ist

$$S/\mathfrak{p}S = S \otimes_R R/\mathfrak{p}$$

ein $R/\mathfrak{p}$-Vektorraum der Dimension n. Oben rechts steht das Produkt der $R/\mathfrak{p}$-Vektorräume $S/\mathfrak{q}_j^{e_j}$ und es ist zu zeigen, dass deren $R/\mathfrak{p}$-Dimension gleich $e_j f_j$ ist. Dies zeigen wir durch Induktion über $e = e_j$, wobei der Induktionsanfang für $e = 1$ die Definition des Trägheitsgrades f_j ist. Wegen $\mathfrak{q}^{e+1} \subseteq \mathfrak{q}^e$ liegt eine kurze exakte Sequenz

$$0 \longrightarrow \mathfrak{q}^e/\mathfrak{q}^{e+1} \longrightarrow S/\mathfrak{q}^{e+1} \longrightarrow S/\mathfrak{q}^e \longrightarrow 0$$

vor. Dabei ist

$$\mathfrak{q}^e/\mathfrak{q}^{e+1} = \mathfrak{q}^e S_{\mathfrak{q}}/\mathfrak{q}^{e+1} S_{\mathfrak{q}} = S_{\mathfrak{q}}/\mathfrak{q}S_{\mathfrak{q}} = S/\mathfrak{q}.$$

Deshalb folgt die Aussage aufgrund der Vektorraumadditivität in kurzen exakten Sequenzen. □

Die in diesem Satz auftretende Gleichung nennt man auch *fundamentale Gleichung*. Nach Lemma 18.3 liegt genau dann Verzweigung oberhalb von $\mathfrak{p}$ vor, wenn einer der Verzweigungsindizes e_j größer als 1 ist.

Die beiden extremen Möglichkeiten für das Zerlegungsverhalten bekommen einen eigenen Namen.

Definition 20.5. Es sei R ein Dedekindbereich mit Quotientenkörper K, $K \subseteq L$ eine Körpererweiterung vom Grad n und S der ganze Abschluss von R in L. Ein von 0 verschiedenes Primideal $\mathfrak{p}$ von R heißt *voll zerlegt* in S, wenn es n Primideale in S oberhalb von $\mathfrak{p}$ gibt.

Im voll zerlegten Fall ist $e_j = f_j = 1$ für $j = 1, \ldots, n$. Es liegt keine Verzweigung von und alle Restekörper stimmen mit dem Grundkörper $R/\mathfrak{p}$ überein.

DEFINITION 20.6. Es sei R ein Dedekindbereich mit Quotientenkörper K, $K \subseteq L$ eine Körpererweiterung vom Grad n und S der ganze Abschluss von R in L. Ein von 0 verschiedenes Primideal $\mathfrak{p}$ von R heißt *unzerlegt* in S, wenn es genau ein Primideal in S oberhalb von $\mathfrak{p}$ gibt.

In diesem Fall ist $n = ef$.

BEISPIEL 20.7. Wir betrachten die Ringerweiterung $\mathbb{R}[X] \subset \mathbb{C}[X]$. Auf der Ebene der Quotientenkörper liegt die quadratische Körpererweiterung der zugehörigen Funktionenkörper $\mathbb{R}(X) \subset \mathbb{C}(X)$ vor, und $\mathbb{C}[X]$ ist der ganze Abschluss von $\mathbb{R}[X]$ in $\mathbb{C}(X)$. Die Primideale $\neq 0$ von $\mathbb{R}[X]$ sind von der Form $(X-a)$ mit $a \in \mathbb{R}$ oder von der Form (X^2+bX+c) mit einem quadratischen Polynom ohne reelle Nullstelle. Die Restekörper in diesem zweiten Fall sind isomorph zu $\mathbb{C}$. Die Primideale in $\mathbb{C}[X]$ sind alle von der Form $(X-a)$ mit $a \in \mathbb{C}$.

In der Erweiterung liegt über dem Primideal $(X-a)$ das entsprechende Ideal, dieses Ideal ist also unzerlegt, die Verzweigungsordnung ist 1 und die Restekörpererweiterung ist $\mathbb{R} \subset \mathbb{C}$, der Trägheitsgrad ist also 2. Zu einem Primideal (X^2+bX+c) zu einem Polynom ohne reelle Nullstelle seien z und $\overline{z}$ die zueinander konjugierten komplexen Nullstellen. In $\mathbb{C}[X]$ gilt die Idealzerlegung $(X^2+bX+c) = (X-z)(X-\overline{z})$. Die Verzweigungsordnungen sind also 1 und in den Restekörpern liegt ein Isomorphismus vor, die Trägheitsgrade sind also 1. Diese Primideale sind voll zerlegt.

BEISPIEL 20.8. Es sei $R = \mathbb{Z}[X]/(X^4+X^3+X^2+X+1) = \mathbb{Z}[x]$. Wir beschreiben exemplarisch das Verhalten von Primzahlen in diesem Zahlbereich. Sei zuerst $q = 5$. Hier ist über $\mathbb{Z}/(5)$

$$(X-1)(X^4+X^3+X^2+X+1) = X^5-1 = (X-1)^5$$

und somit $X^4+X^3+X^2+X+1 = (X-1)^4$. Es gibt also nur ein Primideal oberhalb von (5) und dessen Restklassenkörper ist $\mathbb{Z}/(5)$, der Trägheitsgrad ist also 1 und der Verzweigungsindex ist 4.

Das Zerlegungsverhalten der anderen Primzahlen $q \neq 5$ versuchen wir mit Hilfe eines Zwischenringes zu verstehen. Sei

$$v = x - x^2 - x^3 + x^4.$$

Eine direkte Rechnung (siehe Beispiel 17.5) zeigt $v^2 = 5$, d.h. es liegt ein Zwischenring

$$\mathbb{Z} \subset \mathbb{Z}[\sqrt{5}] \subset \mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \mathbb{Z}[x^3+x^2] = S \subset \mathbb{Z}[x]$$

vor, wobei der Ganzheitsring zu $\sqrt{5}$ mit Satz 9.8 bestimmt wurde.

Für

$$q = 1, 4 \mod 5$$

ist 5 ein Quadrat modulo q. Über diesen Primzahlen liegen in S zwei Primideale, beide mit dem Restekörper $\mathbb{Z}/(q)$ und dem Trägheitsgrad 1. Über

diesen Primzahlen zerfällt das fünfte Kreisteilungspolynom in zwei Faktoren vom Grad 2. Ob es weiter in Linearfaktoren zerfällt, hängt von q ab.

Bei $q = 11$ sind $1, 3, 4, 5, 9$ fünfte Einheitswurzeln in $\mathbb{Z}/(11)$ und das Kreisteilungspolynom hat die Zerlegung

$$X^4 + X^3 + X^2 + X + 1 = (X-3)(X+2)(X-4)(X-5).$$

Über (11) liegen also vier Primideale, jeweils mit dem Trägheitsgrad 1. Ein entsprechendes Verhalten gilt für alle Primzahlen q mit $q = 1 \mod 5$ nach Korollar 23.3.

Bei $q = 4 \mod 5$ gibt es nur die 1 als fünfte Einheitswurzel und es gilt

$$X^4 + X^3 + X^2 + X + 1 = \left(X^2 + \frac{\sqrt{5}+1}{2}X + 1\right)\left(X^2 - \frac{\sqrt{5}-1}{2}X + 1\right),$$

wobei für $\sqrt{5}$ eine Quadratwurzel von 5 aus $\mathbb{Z}/(q)$ einzusetzen ist. Bei $q = 19$ ist beispielsweise $9^2 = 5$ und daher ist

$$X^4 + X^3 + X^2 + X + 1 = \big(X^2 + 5X + 1\big)\big(X^2 + 15X + 1\big).$$

Bei $q = 3 \mod 5$

Es ist einfach Beispiele von Zahlbereichen anzugeben, in denen jedes Primideal des Grundringes zerlegt (also nicht unzerlegt) ist. Für das folgende Beispiel siehe auch Korollar 22.9.

Beispiel 20.9. Es seien $a, b \in \mathbb{Z}$ verschiedene quadratfreie Zahlen, sei

$$\mathbb{Q} \subset L = \mathbb{Q}[\sqrt{a}, \sqrt{b}]$$

die zugehörige Körpererweiterung vom Grad 4 und sei

$$T = \mathbb{Z}[\sqrt{a}, \sqrt{b}] \subseteq S$$

der Ganzheitsring von $\mathbb{Z}$ in L, wobei für dieses Beispiel der Unterschied zwischen T und S irrelevant ist. Wir bestimmen die Faser über einem Primideal zu einer Primzahl p. Der beschreibende Ring ist

$$T \otimes_{\mathbb{Z}} \mathbb{Z}/(p) = \mathbb{Z}[X,Y]/(X^2-a, Y^2-b) \otimes_{\mathbb{Z}} \mathbb{Z}/(p) = \mathbb{Z}/(p)[X,Y]/(X^2-a, Y^2-b).$$

Wir beschränken uns auf Primzahlen ≥ 3, die weder a noch b teilen, was bedeutet, dass die zugehörigen Restklassen Einheiten in $\mathbb{Z}/(p)$ sind. Wenn a (entsprechend für b) ein Quadrat in $\mathbb{Z}/(p)$ ist, sagen wir

$$a = r^2 = (-r)^2,$$

so ist

$$\begin{aligned} & \mathbb{Z}/(p)[X,Y]/(X^2-a, Y^2-b) \\ = \; & \mathbb{Z}/(p)[X,Y]/((X-r)(X+r), Y^2-b) \\ = \; & (\mathbb{Z}/(p)[Y]/(Y^2-b))[X]/((X-r)(X+r)) \\ = \; & (\mathbb{Z}/(p)[Y]/(Y^2-b)) \times (\mathbb{Z}/(p)[Y]/(Y^2-b)), \end{aligned}$$

wobei die letzte Identifizierung durch $X \mapsto (r, -r)$ gegeben ist. Der Faserring ist also ein Produktring und kein Körper und (p) zerfällt in T und dann auch in S in zumindest zwei Primideale.

Wenn hingegen sowohl a als auch b Nichtquadrate in $\mathbb{Z}/(p)$ sind, so ist das Produkt ab ein Quadrat, sagen wir $ab = s^2 = (-s)^2$. Dann gelten, da ja a eine Einheit ist, in $\mathbb{Z}/(p)[X, Y]$ die Idealgleichheiten

$$\begin{aligned}(X^2 - a, Y^2 - b) &= (X^2 - a, aY^2 - ab)\\ &= (X^2 - a, aY^2 - s^2)\\ &= (X^2 - a, X^2Y^2 - s^2)\\ &= (X^2 - a, (XY - s)(XY - s))\end{aligned}$$

und damit ist

$$\begin{aligned}\mathbb{Z}/(p)[X, Y]/(X^2 - a, Y^2 - b) &= \mathbb{Z}/(p)[X, Y]/(X^2 - a, (XY - s)(XY - s))\\ &= (\mathbb{Z}/(p)[X]/(X^2 - a))[Y]/(XY - s)(XY - s)\\ &= (\mathbb{Z}/(p)[X]/(X^2 - a))[Y]/\Big(Y - \frac{s}{X}\Big)\Big(Y - \frac{s}{X}\Big)\\ &= (\mathbb{Z}/(p)[X]/(X^2 - a)) \times (\mathbb{Z}/(p)[X]/(X^2 - a)),\end{aligned}$$

es liegt also wieder ein Produktring vor.

Abbildungsverzeichnis