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

Algebraische Zahlentheorie

Vorlesung 22

Das Zerlegungsverhalten bei Galoiserweiterungen

Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung vom Grad n. Die Galoisgruppe, d.h. die Gruppe der K-Algebraautomorphismen von L, besteht also aus n Automorphismen. Die Untergruppen der Galoisgruppe entsprechen nach dem Satz über die Galoiskorrespondenz den Zwischenkörpern der Erweiterung. Die Galoisgruppe operiert nach Satz 21.2 auch auf dem ganzen Abschluss S von R in L. Hier besprechen wir Untergruppen, ihre zugehörigen Zwischenkörper und Zwischenringe, die mit dem Zerlegungsverhalten von Primidealen unter der Erweiterung $R \subseteq S$ zusammenhängen. Zuerst formulieren wir, wie sich die fundamentale Gleichung aus Satz 20.4 im Galoisfall vereinfacht.

Lemma 22.1. *Es sei R ein Dedekindbereich mit Quotientenkörper K, $K \subseteq L$ eine Galoiserweiterung vom Grad n und sei S der ganze Abschluss von R in L. Es sei $\mathfrak{p}$ ein von 0 verschiedenes Primideal von R. Dann stimmen in der Primidealzerlegung*

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

die Exponenten e_i überein und ebenso stimmen die Trägheitsgrade f_i überein. Dabei ist

$$n = kef.$$

Beweis. Es seien $\mathfrak{q}$ und $\mathfrak{q}'$ Primideale oberhalb von $\mathfrak{p}$. Nach Lemma 21.9 gibt es einen Automorphismus $\sigma \in \operatorname{Gal}(L|K)$ mit $\sigma(\mathfrak{q}) = \mathfrak{q}'$. Daher gibt es einen $R_{\mathfrak{p}}$-Algebraisomorphismus $\sigma\colon S_{\mathfrak{q}} \to S_{\mathfrak{q}'}$, weshalb die Verzweigungsordnungen gleich sind, und einen $\kappa(\mathfrak{p})$-Isomorphismus der Restekörper

$$\kappa(\mathfrak{q}) \longrightarrow \kappa(\mathfrak{q}'),$$

weshalb die Trägheitsgrade gleich sind. Die Formel aus Satz 20.4 nimmt daher die angegebene Gestalt an. □

Es sei $\mathfrak{p}$ ein Primideal aus R und seien $\mathfrak{q}_1, \ldots, \mathfrak{q}_k$ die Primideale von S oberhalb von $\mathfrak{p}$. Gemäß Lemma 21.9 und wie eben verwendet lassen sich diese Primideale ineinander mit isomorphen Restekörpern überführen. Dies bedeutet natürlich nicht, dass der Gruppenhomomorphismus

$$G \longrightarrow \operatorname{Perm}(\mathfrak{q}_1, \ldots, \mathfrak{q}_k)$$

bijektiv ist, wobei rechts die Permutationsgruppe zur Faser über $\mathfrak{p}$ steht. Dabei ist die Bijektivität oft schon wegen der Anzahl ausgeschlossen. Wenn

der Grad n ist, und wenn, im total zerlegten Fall, die Faser aus n Primidealen besteht, so steht links (im Galoisfall) eine Gruppe mit n Elementen und rechts eine Gruppe mit $n!$ Elementen, was nur bei $n \leq 2$ übereinstimmt. Wenn hingegen, im unzerlegten Fall, die Faser aus nur einem Primideal besteht, so steht rechts die triviale Gruppe. Ein Automorphismus $\sigma \in G$ gehört genau dann zum Kern, wenn jedes Primideal der Faser unter σ auf sich selbst abgebildet wird. Diese Bedingung führt, auf ein einzelnes Primideal angewendet, zum Begriff der Zerlegungsgruppe.

DEFINITION 22.2. Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L und sei $\mathfrak{q}$ ein Primideal von S. Dann nennt man

$$G_{\mathfrak{q}} = \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

die *Zerlegungsgruppe* zu $\mathfrak{q}$.

Man spricht auch von der *Isotropiegruppe* oder dem *Stabilisator* zu $\mathfrak{q}$. Man beachte, dass die Bedingung besagt, dass $\mathfrak{q}$ auf sich selbst abgebildet wird, nicht, dass die Einschränkung auf $\mathfrak{q}$ die Identität ist.

LEMMA 22.3. *Es sei R ein Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L und sei $\mathfrak{q}$ ein Primideal von S über $\mathfrak{p}$. Dann gelten folgende Eigenschaften.*

(1) *Die Zerlegungsgruppe $G_{\mathfrak{q}}$ ist genau dann trivial, wenn $\mathfrak{p}$ voll zerlegt ist.*
(2) *Die Zerlegungsgruppe $G_{\mathfrak{q}}$ ist genau gleich G, wenn $\mathfrak{p}$ unzerlegt ist.*
(3) *Zu einem weiteren Primideal $\mathfrak{q}'$ oberhalb von $\mathfrak{p}$ sind die Zerlegungsgruppen $G_{\mathfrak{q}}$ und $G_{\mathfrak{q}'}$ isomorph.*
(4) *Es ist*

$$\#(G_{\mathfrak{q}}) = ef,$$

wobei e der gemeinsame Verzweigungsindex und f der gemeinsame Trägheitsgrad der Primideale oberhalb von $\mathfrak{p}$ ist.

Beweis. (1) und (2) sind klar und folgen auch aus (4).

(3). Nach Lemma 21.9 gibt es ein $\tau \in G$ mit $\tau(\mathfrak{q}) = \mathfrak{q}'$. Mittels τ kann man direkt den Isomorphismus

$$G_{\mathfrak{q}} \longrightarrow G_{\mathfrak{q}'},\ \sigma \longmapsto \tau \circ \sigma \circ \tau^{-1},$$

angeben. Es ist ja

$$\left(\tau \circ \sigma \circ \tau^{-1}\right)(\mathfrak{q}') = \tau(\sigma(\tau^{-1}(\mathfrak{q}'))) = \tau(\sigma(\mathfrak{q})) = \tau(\mathfrak{q}) = \mathfrak{q}'.$$

(4). Wir zerlegen G abhängig davon, auf welches Primideal $\mathfrak{q}$ abgebildet wird, also

$$G = \bigcupplus_{\mathfrak{q}'} \{\rho \in G \mid \rho(\mathfrak{q}) = \mathfrak{q}'\}.$$

Dabei ist die Untergruppe $G_{\mathfrak{q}}$ ein Teil davon und die anderen Teile sind die Nebenklassen zu dieser Untergruppe, da ja

$$\{\rho \in G \mid \rho(\mathfrak{q}) = \mathfrak{q}'\} = \tau G_{\mathfrak{q}},$$

wenn τ ein fixierter Automorphismus ist, der $\mathfrak{q}$ in $\mathfrak{q}'$ überführt. Insbesondere sind diese Nebenklassen alle gleich groß. Wenn es k Primideale in der Faser gibt, und die Körpererweiterung den Grad n hat und die Galoisgruppe somit n Elemente besitzt, so enthält die Zerlegungsgruppe $\frac{n}{k}$ Elemente, was nach Lemma 22.1 mit ef übereinstimmt. □

Definition 22.4. Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L und sei $\mathfrak{q}$ ein Primideal von S. Dann nennt man den Fixkörper zur Zerlegungsgruppe $G_{\mathfrak{q}}$ den *Zerlegungskörper* zu $\mathfrak{q}$. Er wird mit $Z_{\mathfrak{q}}$ bezeichnet.

Den Ganzheitsring zum Zerlegungskörper nennt man *Zerlegungsring*.

Lemma 22.5. *Es sei R ein Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L und sei $\mathfrak{q}$ ein Primideal von S über $\mathfrak{p}$. Dann gelten folgende Eigenschaften.*

(1) *Es gibt einen natürlichen Gruppenhomomorphismus*

$$G_{\mathfrak{q}} \longrightarrow \mathrm{Gal}\,(\kappa(\mathfrak{q})|\kappa(\mathfrak{p})).$$

(2) *Wenn die Erweiterung der Restekörper separabel ist, so handelt es sich bereits um eine Galoiserweiterung, und der Gruppenhomomorphismus ist surjektiv.*
(3) *Wenn $\mathfrak{q}$ zusätzlich unverzweigt ist, so liegt ein Isomorphismus vor.*

Beweis. (1) Sei $\sigma \in G_{\mathfrak{q}}$, also $\sigma^{-1}(\mathfrak{q}) = \mathfrak{q}$. Dies induziert einen Ringautomorphismus (der R fest lässt)

$$\sigma\colon S_{\mathfrak{q}} \longrightarrow S_{\mathfrak{q}}$$

und einen Körperautomorphismus

$$\sigma\colon \kappa(\mathfrak{q}) \longrightarrow \kappa(\mathfrak{q}),$$

der $\kappa(\mathfrak{p})$ fest lässt, also ein Element der Galoisgruppe zur Körpererweiterung $\kappa(\mathfrak{p}) \subseteq \kappa(\mathfrak{q})$. Diese Zuordnung ist insgesamt ein Gruppenhomomorphismus aufgrund der Kommutativität des Diagramms

$$\begin{array}{ccccc} S_{\mathfrak{q}} & \stackrel{\sigma}{\longrightarrow} & S_{\mathfrak{q}} & \stackrel{\tau}{\longrightarrow} & S_{\mathfrak{q}} \\ \downarrow & & \downarrow & & \downarrow \\ \kappa(\mathfrak{q}) & \stackrel{\sigma}{\longrightarrow} & \kappa(\mathfrak{q}) & \stackrel{\tau}{\longrightarrow} & \kappa(\mathfrak{q}) \end{array} .$$

(2) Nach Aufgabe 22.6 können wir davon ausgehen, indem wir K durch den Zerlegungskörper und $\mathfrak{p}$ durch den Schnitt von $\mathfrak{q}$ mit dem Zerlegungsring ersetzen, dass die Zerlegungsgruppe die volle Galoisgruppe ist, dass also $\mathfrak{q}$ das einzige Primideal oberhalb von $\mathfrak{p}$ ist. Aufgrund der Voraussetzung über die Separabilität können wir nach dem Satz vom primitiven Element

$$\kappa(\mathfrak{p}) \subseteq \kappa(\mathfrak{q}) = \kappa(\mathfrak{p})[z]$$

ansetzen, wobei wir unmittelbar $z \in S$ annehmen können. Es sei $P \in R[X]$ das Minimalpolynom von z über R. Es ist also $P(z) = 0$ in S und damit insbesondere $P(z) = 0$ in $\kappa(\mathfrak{q})$. Da $K \subseteq L$ eine Galoiserweiterung ist, zerfällt wegen Satz 16.6 (Körper- und Galoistheorie (Osnabrück 2018-2019)) P in $L[X]$ und damit wegen Satz 21.2 auch in $S[X]$ in Linearfaktoren. Dies gilt dann auch in $\kappa(\mathfrak{q})[X]$ und überträgt sich auf das Minimalpolynom von z über $\kappa(\mathfrak{p})$, was wiederum nach Satz 16.6 (Körper- und Galoistheorie (Osnabrück 2018-2019)) bedeutet, dass die Restekörpererweiterung galoissch ist.

Es sei nun

$$\tau\colon \kappa(\mathfrak{q}) = \kappa(\mathfrak{p})[z] \longrightarrow \kappa(\mathfrak{q}) = \kappa(\mathfrak{p})[z]$$

ein $\kappa(\mathfrak{p})$-Körperautomorphismus, der den Erzeuger z auf ein Element $w \in \kappa(\mathfrak{q})$ schickt, das wir wiederum als repräsentiert durch eine Nullstelle w von P annehmen dürfen. Nach Korollar 15.9 (Körper- und Galoistheorie (Osnabrück 2018-2019)) gehört dazu ein K-Automorphismus von L, der z in w überführt, und dessen Einschränkung stimmt mit τ überein, da er auf einem Erzeuger damit übereinstimmt.

(3) Nach Lemma 22.3 (4) ist im unverzweigten Fall $\#(G_{\mathfrak{q}}) = f$ und dies ist nach Definition der Grad der Körpererweiterung

$$\kappa(\mathfrak{p}) \subseteq \kappa(\mathfrak{q}).$$

Da nach (2) die Restekörpererweiterung galoissch ist, besitzt deren Galoisgruppe ebenfalls f Elemente und deshalb folgt aus der Surjektivität bereits die Bijektivität.

□

Definition 22.6. Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G.

Es sei S der ganze Abschluss von R in L und sei $\mathfrak{q}$ ein Primideal von S. Dann nennt man

$$I_{\mathfrak{q}} = \left\{\sigma \in G_{\mathfrak{q}} \mid \sigma|_{\kappa(\mathfrak{q})} = \mathrm{Id}\right\}$$

die *Trägheitsgruppe* zu $\mathfrak{q}$.

Es liegt also eine Kette von Untergruppen

$$I_{\mathfrak{q}} \subseteq G_{\mathfrak{q}} \subseteq G$$

vor.

Definition 22.7. Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L und sei $\mathfrak{q}$ ein Primideal von S. Dann nennt man den Fixkörper zur Trägheitsgruppe $I_{\mathfrak{q}}$ den *Trägheitskörper* zu $\mathfrak{q}$. Er wird mit $T_{\mathfrak{q}}$ bezeichnet.

Lemma 22.8. *Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L und sei $\mathfrak{q}$ ein Primideal von S. Die Erweiterung der Restekörper sei separabel. Dann ist die Ordnung der Trägheitsgruppe $I_{\mathfrak{q}}$ gleich dem Verzweigungsindex von $\mathfrak{q}$. Insbesondere ist die Trägheitsgruppe genau dann trivial, wenn in $\mathfrak{q}$ keine Verzweigung vorliegt.*

Beweis. Nach Lemma 22.5 (2) liegt eine kurze exakte Sequenz

$$0 \longrightarrow I_{\mathfrak{q}} \longrightarrow G_{\mathfrak{q}} \longrightarrow \mathrm{Gal}\left(\kappa(\mathfrak{q})|\kappa(\mathfrak{p})\right) \longrightarrow 0$$

vor. Die Ordnung der Galoisgruppe rechts ist der Trägheitsgrad f und die Ordnung der Zerlegungsgruppe $G_{\mathfrak{q}}$ ist nach Lemma 22.3 gleich ef, wobei e den Verzweigungsindex bezeichnet. Deshalb ist die Ordnung der Trägheitsgruppe gleich e. □

Wir besprechen weiter Besonderheiten in der zahlentheoretischen Situation, die insbesondere damit zusammenhängen, dass Körpererweiterungen zwischen endlichen Körper zyklisch sind und vom Frobenius (bzw. einer Frobeniuspotenz) erzeugt werden.

Korollar 22.9. *Es sei R ein Zahlbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit einer nicht zyklischen Galoisgruppe G. Dann sind alle Primideale $\mathfrak{p}$ aus R bis auf endlich viele Ausnahmen im ganzen Abschluss von R in L zerlegt.*

Beweis. Es sei $\mathfrak{p}$ nicht verzweigt und sei $\mathfrak{q}$ ein Primideal oberhalb von $\mathfrak{p}$. Nehmen wir an, dass $\mathfrak{p}$ unzerlegt ist, dass also $\mathfrak{q}$ das einzige Primideal darüber ist. Dann liegt nach Lemma 22.5 (3) ein Gruppenisomorphismus

$$G = G_{\mathfrak{q}} \longrightarrow \mathrm{Gal}\left(\kappa(\mathfrak{q})|\kappa(\mathfrak{p})\right)$$

vor. Da die Gruppe rechts nach Satz 5.23 bzw. nach Korollar 16.10 (Körper- und Galoistheorie (Osnabrück 2018-2019)) zyklisch ist, ergibt sich ein Widerspruch zur Voraussetzung. □

BEMERKUNG 22.10. Es sei $R \subseteq S$ eine Erweiterung von Zahlbereichen zu einer Galoiserweiterung $Q(R) = K \subseteq Q(S) = L$ mit Galoisgruppe G. Wenn ein Primideal $\mathfrak{p}$ aus R unverzweigt in S und $\mathfrak{q}$ ein Primideal darüber ist, so liegt nach Lemma 22.5 (3) ein kanonischer Isomorphismus zwischen der Zerlegungsgruppe $G_{\mathfrak{q}}$ und der zyklischen Galoisgruppe $\mathrm{Gal}\,(\kappa(\mathfrak{q})|\kappa(\mathfrak{p}))$, die vom Frobenius bzw. einer Frobeniuspotenz (siehe Korollar 16.10 (Körper- und Galoistheorie (Osnabrück 2018-2019))) erzeugt wird. Man nennt daher auch den entsprechenden Erzeuger der Zerlegungsgruppe $G_{\mathfrak{q}}$ den *Frobenius*. Dafür schreibt man

$$(\mathfrak{q}, L/K)$$

und spricht vom Frobenius. Es ist also $(\mathfrak{q}, L/K) \in G_{\mathfrak{q}} \subseteq G$, und man betrachtet diesen Frobenius als Element der Galoisgruppe. Wenn $\mathfrak{q}'$ ein weiteres Primideal über $\mathfrak{p}$ ist, so sind nach Lemma 22.3 die Zerlegungsgruppen über

$$G_{\mathfrak{q}} \longrightarrow G_{\mathfrak{q}'},\ \sigma \longmapsto \tau \circ \sigma \circ \tau^{-1},$$

zueinander isomorph und zwar konjugiert in G. Insbesondere sind dann die Frobenii zueinander konjugiert und bilden eine Konjugationsklasse. Wenn zusätzlich eine abelsche Erweiterung vorliegt, so stimmen diese Frobenius-Automorphismen überein und hängen nur von dem Primideal $\mathfrak{p}$ aus R ab. Man bezeichnet diesen Frobenius mit $(\mathfrak{p}, L/K)$ und spricht vom *Artinsymbol*.

Nikolai Grigorjewitsch Tschebotarjow (1894-1947)

Der *Dichtigkeitssatz von Tschebotarjowsch* besagt, dass bei einer Galoiserweiterung $\mathbb{Q} \subseteq L$ mit (der Einfachheit halber kommutativen) Galoisgruppe G die Menge der Primzahlen, für die ein bestimmtes Gruppenelement $g \in G$ der Frobenius ist, gleichverteilt ist. Insbesondere ist die „Wahrscheinlichkeit“, dass die Identität der Frobenius ist, was ja einfach bedeutet, dass die Zerlegungsgruppe trivial ist, was wiederum nach Lemma 22.3 (1) bedeutet, dass p voll zerlegt ist, gleich $1/\#\,(G)$ ist.

Abbildungsverzeichnis