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

Algebraische Zahlentheorie

Vorlesung 21

Invariantenringe

Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und $\mathbb{Z} \subseteq R$ der zugehörige Zahlbereich. Welche Besonderheiten gelten für R, wenn die Körpererweiterung eine Galoiserweiterung ist, wenn also die Anzahl der $\mathbb{Q}$-Algebraautomorphismen von L mit dem Grad der Erweiterung übereinstimmt. Wir werden gleich sehen, dass die Körperautomorphismen auf R Ringautomorphismen induzieren und dass daher die Galoisgruppe auch auf R operiert. Dies bewirkt, dass es auf R bzw. $\operatorname{Spek}(R)$ Symmetrien gibt. Wir fixieren einige Sprechweisen. Unter der Operation einer Gruppe G auf einem kommutativen Ring als Gruppe von Ringautomorphismen versteht man einen Gruppenhomomorphismus $G \to \operatorname{Aut} R$.

Definition 21.1. Es sei G eine Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen operiert (von rechts). Dann bezeichnet man

$$R^G = \{f \in R \mid f\sigma = f \text{ für alle } \sigma \in G\}$$

als den *Invariantenring* (oder *Fixring*) von R unter der Operation von G.

Dies ist eine Verallgemeinerung des aus der Galoistheorie bekannten Konzeptes eines Fixkörpers. Eine endliche Körpererweiterung ist nach Satz 16.6 (Körper- und Galoistheorie (Osnabrück 2018-2019)) genau dann galoissch, wenn der Fixkörper von L unter der Operation der Galoisgruppe $\operatorname{Gal}(L|K)$ gleich K ist.

Satz 21.2. *Es sei R ein normaler Integritätsbereich mit Quotientenkörper K und sei $K \subseteq L$ eine Galoiserweiterung. Es sei S der ganze Abschluss von R in L. Dann operiert die Galoisgruppe $G = \operatorname{Gal}(L|K)$ auf S mit Invariantenring R.*

Beweis. Es sei $\sigma \in G$ und $f \in S$. Es sei

$$0 = f^n + r_{n-1}f^{n-1} + \cdots + r_2f^2 + r_1f + r_0$$

eine Ganzheitsgleichung für f über R. Dann ist

$$\begin{aligned} 0 &= \sigma\big(f^n + r_{n-1}f^{n-1} + \cdots + r_2f^2 + r_1f + r_0\big) \\ &= \sigma(f)^n + \sigma(r_{n-1})\sigma(f)^{n-1} + \cdots + \sigma(r_2)\sigma(f)^2 + \sigma(r_1)\sigma(f) + \sigma(r_0) \\ &= \sigma(f)^n + r_{n-1}\sigma(f)^{n-1} + \cdots + r_2\sigma(f)^2 + r_1\sigma(f) + r_0 \end{aligned}$$

und somit erfüllt auch $\sigma(f)$ eine Ganzheitsgleichung über R, also $\sigma(f) \in S$. Deshalb lässt sich σ zu einer Abbildung von S nach S einschränken.

Die Gleichheit $S \cap K = R$ ist klar, da R als normal vorausgesetzt wird. Deshalb ist

$$S^G \subseteq S \cap L^G = S \cap K = R,$$

die umgekehrte Inklusion $R \subseteq S^G$ ist klar. $\square$

Korollar 21.3. *Es sei $\mathbb{Q} \subseteq K$ eine Galoiserweiterung und $\mathbb{Z} \subseteq R$ die zugehörige Erweiterung der Zahlbereiche. Dann operiert die Galoisgruppe G auf R mit Invariantenring $R^G = \mathbb{Z}$.*

Beweis. Dies folgt direkt aus Satz 21.2. $\square$

Beispiel 21.4. Eine quadratische Körpererweiterung $\mathbb{Q} \subseteq L = \mathbb{Q}[\sqrt{D}]$ mit einer quadratfreien ganzen Zahl $D \neq 0, 1$ ist stets eine Galoiserweiterung, wobei die Galoisgruppe neben der Identität aus der Konjugation $\sqrt{D} \mapsto -\sqrt{D}$ besteht. Diese Konjugation wirkt nach Satz 21.2 oder direkt nach Aufgabe 9.3 und Aufgabe 9.5 auch auf dem zugehörigen quadratischen Zahlbereich, mit $\mathbb{Z}$ als Invriantenring.

Wir beschreiben nun generell Eigenschaften von Invariantenringen zu einer Operation einer endlichen Gruppe.

Proposition 21.5. *Es sei G eine Gruppe, die auf einem Integritätsbereich R als Gruppe von Ringautomorphismen operiere. Dann gelten folgende Eigenschaften.*

(1) *Der Invariantenring R^G ist ein Integritätsbereich.*
(2) *Die Operation induziert eine Operation von G auf dem Quotientenkörper $Q(R)$ als Gruppe von Körperautomorphismen.*
(3) *Es ist $Q\big(R^G\big) \subseteq (Q(R))^G$.*
(4) *Es ist*

$$R \cap (Q(R))^G = R^G.$$

Beweis. (1) ist wegen $R^G \subseteq R$ klar. (2). Es sei $K = Q(R)$ der Quotientenkörper von R. Zu jedem $\sigma \in G$ setzt sich der Ringautomorphismus $f \mapsto f\sigma$ aufgrund der universellen Eigenschaft der Nenneraufnahme zu einem Körperautomorphismus $\frac{f}{g} \mapsto \frac{f\sigma}{g\sigma}$ fort. (3). Ein Element aus dem Quotientenkörper $Q\big(R^G\big)$ hat die Form $\frac{f}{g}$ mit invarianten Elementen $f, g \in R^G$. Es ist also insbesondere invariant unter der induzierten Operation auf K. Daher gilt $Q\big(R^G\big) \subseteq (Q(R))^G$. (4). Die Inklusion $R^G \subseteq R \cap Q(R)^G$ ist direkt klar. Die andere Inklusion ergibt sich, da die Operation von G auf $Q(R)$ eingeschränkt auf R die ursprüngliche Operation ist. Wenn also $f \in R$ ist und aufgefasst in $Q(R)$ invariant ist, so ist es überhaupt invariant. $\square$

Bei einer endlichen Gruppe gilt in Proposition 21.5 (3) sogar Gleichheit, wie die folgende Aussage zeigt.

Lemma 21.6. *Es sei G eine endliche Gruppe, die auf einem Integritätsbereich als Gruppe von Ringautomorphismen operiere. Dann ist*

$$Q\left(R^G\right) = (Q(R))^G.$$

Beweis. Die Inklusion $Q\left(R^G\right) \subseteq (Q(R))^G$ gilt nach Proposition 21.5 (3) für jede Gruppe. Zum Beweis der Umkehrung seien $f, g \in R$, $g \neq 0$, mit $\frac{f}{g} \in (Q(R))^G$ gegeben. Wir betrachten

$$h = \prod_{\sigma \in G,\, \sigma \neq e_G} g\sigma.$$

Dann gelten in $Q(R)$ die Identitäten

$$\begin{aligned} \frac{f}{g} &= \frac{hf}{hg} \\ &= \frac{hf}{\left(\prod_{\sigma \in G,\, \sigma \neq e_G} g\sigma\right) g} \\ &= \frac{hf}{\prod_{\sigma \in G} g\sigma}. \end{aligned}$$

Nach Voraussetzung ist der Bruch und in dieser Darstellung offenbar auch der Nenner (siehe Aufgabe 21.7) invariant. Also muss auch der Zähler invariant sein und somit ist $\frac{f}{g} \in \left(R^G\right)$. □

Lemma 21.7. *Es sei R ein kommutativer Ring, auf dem eine endliche Gruppe G durch Ringautomorphismen operiere. Dann ist $R^G \subseteq R$ eine ganze Erweiterung.*

Beweis. Zu $f \in R$ betrachten wir das Produkt

$$P = \prod_{\sigma \in G} (X - f\sigma) \in R[X].$$

Die Koeffizienten dieses Polynoms gehören zum Invariantenring R^G. Ferner ist P normiert und es ist $P(f) = 0$ (da ja $X - fe_G = X - f$ ein Linearfaktor ist). Somit liefert P eine Ganzheitsgleichung für f über R^G und daher ist $R^G \subseteq R$ ganz. □

Invariantenring und Quotientenraum

Es sei R ein kommutativer Ring, G eine endliche Gruppe, die auf R als Gruppe von Ringautomorphismen und damit nach Proposition 5.1 auch auf $X = \operatorname{Spek}(R)$ als Gruppe von Homöomorphismen operiere. Dann hat man einerseits den topologischen Quotienten X/G und andererseits den Invariantenring R^G und damit dessen Spektrum $\operatorname{Spek}\left(R^G\right)$. Der topologische Quotient ist einfach der Bahnenraum versehen mit der Bildtopologie. Wir zeigen nach einigen Vorbereitungen, dass diese zwei geometrischen Objekte gleich sind, also dass

$$X/G = \text{Spek}\left(R^G\right)$$

gilt. Dabei werden wir zeigen, dass die Spektrumsabbildung

$$\iota^* \colon \text{Spek}(R) \longrightarrow \text{Spek}\left(R^G\right)$$

(die zur Inklusion $R^G \subseteq R$ gehört) die Eigenschaften eines topologischen Quotienten erfüllt.

Korollar 21.8. *Es sei R ein kommutativer Ring, auf dem eine endliche Gruppe G durch Ringautomorphismen operiere. Dann ist die Spektrumsabbildung*

$$\iota^* \colon \text{Spek}(R) \longrightarrow \text{Spek}\left(R^G\right)$$

surjektiv und abgeschlossen. Insbesondere trägt $\text{Spek}\left(R^G\right)$ *die Bildtopologie unter dieser Abbildung.*

Beweis. Dies folgt aus Lemma 21.7 und aus Satz Anhang 5.3. □

Lemma 21.9. *Es sei R ein kommutativer Ring, auf dem eine endliche Gruppe G durch Ringautomorphismen operiere und es sei*

$$\iota^* \colon \text{Spek}(R) \longrightarrow \text{Spek}\left(R^G\right)$$

die zugehörige Spektrumsabbildung. Dann gilt für $\mathfrak{p}, \mathfrak{q} \in \text{Spek}(R)$ die Äquivalenz: $\iota^*(\mathfrak{p}) = \iota^*(\mathfrak{q})$ genau dann, wenn es ein $\sigma \in G$ mit $\sigma^*(\mathfrak{p}) = \mathfrak{q}$ gibt. Das heißt, dass die Bahnen der Operation von G auf $\text{Spek}(R)$ mit den Fasern von ι^* übereinstimmen.

Beweis. Wenn $\sigma^*(\mathfrak{p}) = \sigma^{-1}(\mathfrak{p}) = \mathfrak{q}$ ist und $f \in R^G \cap \mathfrak{q}$, so ist auch $f = f\sigma \in \mathfrak{p}$, also ist

$$\iota^*(\mathfrak{p}) = R^G \cap \mathfrak{p} = R^G \cap \mathfrak{q} = \iota^*(\mathfrak{q}).$$

Primideale in derselben Bahn besitzen also den gleichen Bildpunkt unter der Spektrumsabbildung.

Zum Beweis der Umkehrung betrachten wir die Faser über $\mathfrak{r} \in \text{Spek}\left(R^G\right)$ und es sei $\mathfrak{p}$ ein Element dieser Faser, welches es nach Korollar 21.8 gibt. Wir müssen zeigen, dass jedes Primideal $\mathfrak{q}$ der Faser in der Bahn durch $\mathfrak{p}$ liegt, dass es also ein $\sigma \in G$ mit $\sigma^*(\mathfrak{p}) = \mathfrak{q}$ gibt. Wir nehmen an, dass dies nicht der Fall sei, und es sei $\mathfrak{q}$ ein Primideal der Faser über $\mathfrak{r}$, das aber nicht zur Bahn durch $\mathfrak{q}$ gehört. Aus $\mathfrak{q} \neq \sigma^*(\mathfrak{p})$ (für alle $\sigma \in G$) folgt $\mathfrak{q} \not\subseteq \sigma^*(\mathfrak{p})$, da andernfalls die Faser im Widerspruch zu Lemma Anhang 5.5 nicht nulldimensional wäre. Nach Lemma 11.10 (Kommutative Algebra) ist dann auch

$$\mathfrak{q} \not\subseteq \bigcup_{\sigma \in G} \sigma^*(\mathfrak{p}) =: T.$$

Sei $f \in \mathfrak{q}$, $f \notin T$. Die Menge T wird unter der Gruppenoperation auf sich selbst abgebildet, daher ist auch $f\sigma \notin T$. Somit ist auch $g = \prod_{\sigma \in G} f\sigma \notin T$.

Andererseits ist aber $g \in R^G$ und $g \in \mathfrak{q}$, also ergibt sich der Widerspruch $g \in R^G \cap \mathfrak{q} = \mathfrak{r} \subseteq \mathfrak{p} \subseteq T$. □

Satz 21.10. *Es sei R ein kommutativer Ring, auf dem eine endliche Gruppe G durch Ringautomorphismen operiere und es sei*

$$\iota^* \colon \operatorname{Spek}(R) \longrightarrow \operatorname{Spek}\left(R^G\right)$$

die zugehörige Spektrumsabbildung. Dann ist $\left(\operatorname{Spek}\left(R^G\right), \iota^*\right)$ der Quotient der Gruppenoperation von G auf $\operatorname{Spek}(R)$.

Beweis. Die Abbildung

$$\iota^* \colon \operatorname{Spek}(R) \longrightarrow \operatorname{Spek}\left(R^G\right)$$

ist nach Korollar 21.8 surjektiv, so dass nach Lemma 21.9 die Punkte aus $\operatorname{Spek}\left(R^G\right)$ den Bahnen der Gruppenoperation entsprechen. Daher ist Spek $\left(R^G\right)$ ein mengentheoretischer Quotient. Nach Korollar 21.8 trägt $\operatorname{Spek}\left(R^G\right)$ die Bildtopologie, so dass es sich auch um einen topologischen Quotienten handelt. □

Korollar 21.11. *Es sei $\mathbb{Q} \subseteq K$ eine Galoiserweiterung und $\mathbb{Z} \subseteq R$ die zugehörige Erweiterung der Zahlbereiche. Es sei $p \in \mathbb{Z}$ eine Primzahl und seien $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec}(R)$ Primideale oberhalb von (p). Dann sind die lokalen Ringe $R_{\mathfrak{p}}$ und $R_{\mathfrak{q}}$ und die Restekörper $\kappa(\mathfrak{p})$ und $\kappa(\mathfrak{q})$ zueinander isomorph.*

Beweis. Nach Korollar 21.3 ist $R^G = \mathbb{Z}$. Wenn $\mathfrak{p}$ und $\mathfrak{q}$ auf das gleiche Primideal in $\mathbb{Z}$ runterschneiden, so gibt es nach Lemma 21.9 einen Automorphismus

$$\sigma \colon R \longrightarrow R$$

mit $\sigma^{-1}(\mathfrak{p}) = \mathfrak{q}$. Dazu gehört ein Isomorphismus

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

und ein Isomorphismus der Restekörper. □

Abbildungsverzeichnis