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

Algebraische Zahlentheorie

Vorlesung 5

Das Spektrum unter Ringhomomorphismen

Wir untersuchen, wie sich das Spektrum eines kommutativen Ringes unter einem Ringhomomorphismus verhält.

PROPOSITION 5.1. *Es sei $\varphi\colon R \to S$ ein Ringhomomorphismus zwischen kommutativen Ringen. Dann gelten folgende Aussagen.*

(1) *Die Zuordnung*

$$\varphi^*\colon \operatorname{Spek}(S) \longrightarrow \operatorname{Spek}(R),\ \mathfrak{p} \longmapsto \varphi^*(\mathfrak{p}) := \varphi^{-1}(\mathfrak{p}),$$

ist (wohldefiniert und) stetig.

(2) *Es ist $(\varphi^*)^{-1}(D(\mathfrak{a})) = D(\mathfrak{a}S)$ für jedes Ideal $\mathfrak{a} \subseteq R$.*

(3) *Für einen weiteren Ringhomomorphismus*

$$\psi\colon S \longrightarrow T$$

gilt $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.

Beweis. Die Abbildung ist nach Aufgabe 5.1 wohldefiniert. Zur Stetigkeit ist die Aussage (2) zu zeigen. Wir argumentieren mit den abgeschlossenen Mengen. Für ein Primideal $\mathfrak{q} \in \operatorname{Spek}(S)$ ist $\varphi^*(\mathfrak{q}) \in V(\mathfrak{a})$ genau dann, wenn $\mathfrak{a} \subseteq \varphi^{-1}(\mathfrak{q})$ ist. Dies ist äquivalent zu $\varphi(\mathfrak{a}) \subseteq \mathfrak{q}$ und ebenso zu $\mathfrak{a}S \subseteq \mathfrak{q}$. (3) ist klar. □

Die in der vorstehenden Aussage eingeführte stetige Abbildung heißt *Spektrumsabbildung* (zu dem gegebenen Ringhomomorphismus). Bei einem Unterring

$$R \subseteq S$$

geht es einfach um die Zuordnung $\mathfrak{p} \mapsto \mathfrak{p} \cap R$. In diesem Fall spricht man auch von „Runterschneiden“.

BEISPIEL 5.2. Es sei K ein Körper und $P \in K[X]$ ein Polynom in einer Variablen. Wir betrachten den zugehörigen Ringhomomorphismus

$$K[Y] \longrightarrow K[X],\ Y \longmapsto P.$$

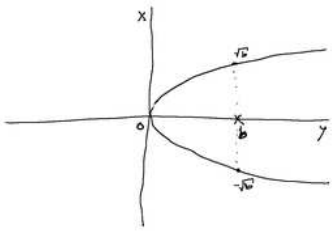
Das Urbild zu einem linearen Primideal $(X - a) \in K[X]$ ist das Primideal $(Y - P(a)) \in K[Y]$. Dies sieht man am einfachsten, wenn man die Hintereinanderschaltung

$$K[Y] \longrightarrow K[X] \xrightarrow{\mathrm{Ev}_a} K$$

betrachtet, die die Evaluation an $P(a)$ ist, und die Kerne beachtet. Deshalb liegt das kommutatives Diagramm

$$\begin{array}{rcl} K & \longrightarrow & \mathrm{Spek}\,(K[X]) \\ P\downarrow & & \downarrow \\ K & \longrightarrow & \mathrm{Spek}\,(K[Y]) \end{array}$$

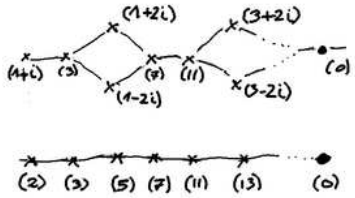
vor, wobei in den Horizontalen die Zuordnungen $a \mapsto (X-a)$ bzw. $b \mapsto (Y-b)$ stehen und rechts die Spektrumsabbildung steht. Die Spektrumsabbildung ist also eine natürliche Erweiterung der durch das Polynom P direkt definierten Abbildung von K nach K, die zusätzlich noch alle Primideale berücksichtigt.



Sieht aus wie die Wurzel, soll aber die Quadrierung sein. Die Quadratabbildung sieht man, wenn man ausgehend von der hier vertikalen x-Achse horizontal auf den Graphen geht und dann nach unten projiziert. Diese Sichtweise betont, wie die Fasern zu variierendem b aussieht.

Im zahlentheoretischen Kontext betrachtet man meist eine Ringerweiterung $\mathbb{Z} \subseteq R$, ein Primideal aus R wird dabei unter der Spektrumsabbildung entweder auf das Nullideal (0) abgebildet oder aber auf ein Primhauptideal (p) zu einer Primzahl p. Diese Abbildung kann man auf zwei Arten versuchen zu verstehen, erstens, indem man die Primideale von R versucht zu verstehen und dann zu bestimmen, wohin diese abgebildet werden, oder aber zweitens, und dies ist im zahlentheoretischen Kontext produktiver, dadurch, dass man versucht zu verstehen, welche Primideale oberhalb von (p) liegen. Diese Frage hängt unmittelbar mit der Frage zusammen, was mit der Primzahl p in der Ringerweiterung R geschieht, ob es eine Primzahl bleibt oder ob und wie es zerfällt. Die Faser über (p) ist direkt (siehe unten) die Menge der Primideale des Restklassenringes $R/(p)$, und dies ist bei einer ganzen Erweiterung ein endlicher Ring.

Beispiel 5.3. Zur Erweiterung $\mathbb{Z} \subseteq \mathbb{Z}[\mathrm{i}]$ stellt man sich die Spekrumsabbildung $\mathrm{Spek}\,(\mathbb{Z}[\mathrm{i}]) \to \mathrm{Spek}\,(\mathbb{Z})$ so vor, dass man zu einer Primzahl $p \in \mathbb{Z}$ versucht zu verstehen, welche Primideale in $\mathbb{Z}[\mathrm{i}]$ die Zahl p enthalten. Dabei entsteht das Bild unten.



PROPOSITION 5.4. *Es sei R ein kommutativer Ring. Dann gelten folgende Aussagen.*

(1) *Zu einem Ideal $\mathfrak{a} \subseteq R$ und der Restklassenabbildung*

$$q\colon\ R \longrightarrow R/\mathfrak{a}$$

ist die Spektrumsabbildung

$$q^*\colon\ \operatorname{Spek}(R/\mathfrak{a}) \longrightarrow \operatorname{Spek}(R)$$

eine abgeschlossene Einbettung, deren Bild $V(\mathfrak{a})$ ist.

(2) *Zu einem multiplikativen System $M \subseteq R$ ist die zur kanonischen Abbildung*

$$\iota\colon\ R \longrightarrow R_M$$

gehörige Abbildung

$$\iota^*\colon\ \operatorname{Spek}(R_M) \longrightarrow \operatorname{Spek}(R)$$

injektiv, und das Bild besteht aus der Menge der Primideale von R, die zu M disjunkt sind.

(3) *Zu $f \in R$ ist die zur kanonischen Abbildung*

$$\iota\colon\ R \longrightarrow R_f$$

gehörige Abbildung

$$\iota^*\colon\ \operatorname{Spek}(R_f) \longrightarrow \operatorname{Spek}(R)$$

eine offene Einbettung, deren Bild gleich $D(f)$ ist.

Beweis. (1) folgt aus Aufgabe 3.13: Die Primideale in $R/\mathfrak{a}$ entsprechen über $\mathfrak{p} \mapsto q^{-1}(\mathfrak{p}) = \mathfrak{p} + \mathfrak{a}$ den Primidealen von R, die $\mathfrak{a}$ enthalten. Die angegebene Abbildung ist also bijektiv und hat das beschriebene Bild. Zu einem Ideal $\mathfrak{b} \subseteq R/\mathfrak{a}$ und einem Primideal $\mathfrak{p} \subseteq R/\mathfrak{a}$ ist genau dann $\mathfrak{b} \subseteq \mathfrak{p}$, wenn

$$\mathfrak{b} + \mathfrak{a} \;=\; q^{-1}(\mathfrak{b}) \;\subseteq\; \mathfrak{p} + \mathfrak{a}$$

gilt. Also ist das Bild von $V(\mathfrak{b})$ gleich $V(\mathfrak{b}+\mathfrak{a})$ und damit abgeschlossen. Für (2) siehe Aufgabe 4.18. (3). Da für ein Primideal $\mathfrak{p}$ und ein Element $f \in R$ die Beziehung $f \notin \mathfrak{p}$ genau dann gilt, wenn $\mathfrak{p}$ zum multiplikativen System $\{f^n \mid n \in \mathbb{N}\}$ disjunkt ist, folgt aus Teil (2), dass die Abbildung injektiv ist und dass ihr Bild gleich $D(f)$ ist. Das gleiche Argument, angewendet auf

$g \in R$ bzw. $\frac{g}{1} \in R_f$ zeigt, dass das Bild von $D(g) \subseteq \operatorname{Spek}(R_f)$ gleich $D(fg)$ und damit offen ist. $\square$

LEMMA 5.5. *Es sei $\varphi\colon R \to S$ ein Ringhomomorphismus zwischen zwei kommutativen Ringen und es sei*

$$\varphi^*\colon \operatorname{Spek}(S) \longrightarrow \operatorname{Spek}(R),\ \mathfrak{p} \longmapsto \varphi^*(\mathfrak{p}),$$

die zugehörige Spektrumsabbildung. Dann ist die Faser über einem Primideal $\mathfrak{q} \in \operatorname{Spek}(R)$ gleich $\operatorname{Spek}\left((S/\mathfrak{q}S)_{\varphi(R\setminus\mathfrak{q})}\right)$. D.h. die Faser besteht aus allen Primidealen $\mathfrak{p} \in \operatorname{Spek}(S)$ mit $\mathfrak{q}S \subseteq \mathfrak{p}$ und mit $\mathfrak{p} \cap \varphi(R \setminus \mathfrak{q}) = \emptyset$.

Beweis. Aufgrund von Proposition 5.4 müssen wir nur die zweite Formulierung beweisen. Für ein Primideal $\mathfrak{p} \subseteq S$ gilt $\varphi^{-1}(\mathfrak{p}) = \mathfrak{q}$ genau dann, wenn sowohl $\varphi(\mathfrak{q}) \subseteq \mathfrak{p}$ als auch $\varphi(R \setminus \mathfrak{q}) \subseteq S \setminus \mathfrak{p}$ gilt. Die erste Bedingung ist zu $\mathfrak{q}S \subseteq \mathfrak{p}$ und die zweite Bedingung ist zu

$$\varphi(R \setminus \mathfrak{q}) \cap \mathfrak{p} = \emptyset$$

äquivalent. $\square$

Insbesondere ist die Faser eines Spektrumsmorphismus über einem Punkt selbst wieder das Spektrum eines Ringes. Ein Spezialfall der vorstehenden Aussage ist, dass die Faser über einem maximalen Ideal $\mathfrak{m}$ gleich $\operatorname{Spek}(S/\mathfrak{m}S)$ ist, da in diesem Fall aus $\mathfrak{m}S \subseteq \mathfrak{p}$ sofort $\mathfrak{m} \subseteq \varphi^{-1}(\mathfrak{p})$ folgt und wegen der Maximalität Gleichheit gelten muss. Bei einem Integritätsbereich R und dem Nullideal erübrigt es sich, das Erweiterungsideal zu betrachten, die Faser wird einfach durch $\operatorname{Spek}\left(S_{\varphi(R\setminus\{0\})}\right)$ beschrieben.

DEFINITION 5.6. Zu einem Ringhomomorphismus $\varphi\colon R \to S$ zwischen kommutativen Ringen und einem Primideal $\mathfrak{q} \in \operatorname{Spek}(R)$ nennt man

$$(S/\mathfrak{q}S)_{\varphi(R\setminus\mathfrak{q})}$$

den *Faserring* über $\mathfrak{q}$.

Die Aussage Lemma 5.5 bedeutet also, dass die Faser der Spektrumsabbildung über $\mathfrak{q}$ gleich dem Spektrum des Faserringes ist. Der Faserring beinhaltet dabei eine genauere algebraische Information, aus der die topologische und mengentheoretische Information ablesbar ist. Wenn $\mathfrak{q}$ ein maximales Ideal von R ist, so braucht man die Nenneraufnahme nicht, der Faserring ist dann einfach gleich $S/\mathfrak{q}S$. Den Faserring kann man allgemein auch als $S \otimes_R \kappa(\mathfrak{q})$ realisieren.

BEMERKUNG 5.7. Wenn ein Ringhomomorphismus in der Form

$$R \longrightarrow R[X_1, \ldots, X_n]/(F_1, \ldots, F_s)$$

vorliegt, so wird der Faserring über einem Primideal $\mathfrak{q} \in \operatorname{Spek}(R)$ durch

$$\left(R/\mathfrak{q}[X_1, \ldots, X_n]/(\overline{F}_1, \ldots, \overline{F}_s)\right)_{\varphi(R\setminus\mathfrak{q})}$$

beschrieben, wobei $\overline{F}_j$ die Reduktion von F_j modulo $\mathfrak{q}$ bezeichnet. Dies bedeutet einfach, dass man die Koeffizienten der Polynome modulo $\mathfrak{q}$ interpretiert.

Bei $R = \mathbb{Z}$ und $S = \mathbb{Z}[X]/(F)$ und einem maximalen Ideal (p) zu einer Primzahl p ist der Faserring einfach $\mathbb{Z}/(p)[X]/(\overline{F})$. Dies ist also eine Algebra über dem endlichen Körper $\mathbb{Z}/(p)$. Wenn F ein normiertes Polynom vom Grad d ist, so ist diese Algebra endlich mit p^d Elementen, die man allein schon wegen der Endlichkeit explizit beschreiben kann. Wenn F über $\mathbb{Z}$ irreduzibel ist, so muss aber $\overline{F}$ nicht unbedingt irreduzibel sein. In der Tat ist es so, dass p genau dann ein Primelement in S bleibt, wenn $\overline{F}$ irreduzibel in $(\mathbb{Z}/(p))[X]$ ist. Genau in diesem Fall ist der Faserring ein Körper.

Endliche Körpererweiterungen

Wir rekapitulieren nun die wichtigsten Ergebnisse der Körper- und Galoistheorie. In der Zahlentheorie geht man von einer endlichen Körpererweiterung $\mathbb{Q} \subseteq L$ aus, wobei L typischerweise durch die Hinzunahme gewisser algebraischer Zahlen definiert ist, und überlegt dann, was dies für die „entsprechende“ Erweiterung für $\mathbb{Z}$ bedeutet. Dabei greift man immer wieder auf die Körpererweiterung zurück.

Definition 5.8. Seien R und A kommutative Ringe und sei $R \to A$ ein fixierter Ringhomomorphismus. Dann nennt man A eine *R-Algebra*.

Jeder Ring ist in eindeutiger Weise eine $\mathbb{Z}$-Algebra. Der Polynomring $K[X]$ ist eine K-Algebra. Wenn ein Unterring $R \subseteq S$ vorliegt, so ist insbesondere S eine R-Algebra. Bei eine Unterringbeziehung $K \subseteq L$ zwischen Körpern spricht man von einem Unterkörper und einem Erweiterungskörper.

Definition 5.9. Sei L ein Körper und $K \subseteq L$ ein Unterkörper von L. Dann heißt L ein *Erweiterungskörper* (oder *Oberkörper*) von K und die Inklusion $K \subseteq L$ heißt eine *Körpererweiterung*.

Bei einer R-Algebra A ist A insbesondere ein R-Modul, siehe Aufgabe 5.10. Speziell ist bei einer Körpererweiterung $K \subseteq L$ der Erweiterungskörper L ein K-Vektorraum. Dies erlaubt es, Begriffe aus der linearen Algebra in dieser Situation anzuwenden.

Definition 5.10. Eine Körpererweiterung $K \subseteq L$ heißt *endlich*, wenn L ein endlichdimensionaler Vektorraum über K ist.

Definition 5.11. Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann nennt man die K-(Vektorraum-)Dimension von L den *Grad* der Körpererweiterung.

Der Grad einer endlichen Körpererweiterung $K \subseteq L$ wird mit

$$\operatorname{grad}_K L$$

bezeichnet. Dass man hier von Grad spricht und nicht einfach von Dimension hat seinen Grund darin, dass dieser Grad mit dem Grad von gewissen Polynomen zusammenhängt, worauf wir ausführlich zu sprechen kommen werden. Da bei einer Körpererweiterung $K \subseteq L$ sofort eine K-Vektorraumstruktur auf L zur Verfügung steht, ist es naheliegend, für das Studium der Körpererweiterungen die lineare Algebra einzusetzen. Dies ist besonders bei endlichen Körpererweiterungen ein schlagkräftiges Mittel. Durch diesen Apparat wird unter Anderem die additive Struktur auf L einfach beschreibbar, und man kann sich ganz auf die Multiplikation konzentrieren. Aber auch für diese ist die Vektorraumstruktur reich an Konsequenzen. Um ein typisches Beispiel für die lineare Argumentationsweise zu geben, betrachten wir eine endliche Körpererweiterung $K \subseteq L$ und ein beliebiges Element $x \in L$. Die Potenzen von x, also

$$x^0 = 1, x^1 = x, x^2, x^3, \ldots$$

bilden eine unendliche Familie (auch wenn es unter den Potenzen Wiederholungen geben kann). Da diese Potenzen alle zu L gehören und L ein endlichdimensionaler K-Vektorraum ist, kann diese unendliche Familie nicht linear unabhängig sein, sondern es muss eine Beziehung der Form

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$$

geben, bei der nicht alle Koeffizienten $a_i \in K$ gleich 0 sind. Diese Beobachtung führt zu den Begriffen *algebraisches Element* und *Minimalpolynom*.

Definition 5.12. Es sei K ein Körper und A eine kommutative K-Algebra. Es sei $f \in A$ ein Element. Dann heißt f *algebraisch* über K, wenn es ein von 0 verschiedenes Polynom $P \in K[X]$ mit $P(f) = 0$ gibt.

Definition 5.13. Es sei K ein Körper und A eine K-Algebra. Es sei $f \in A$ ein über K algebraisches Element. Dann heißt das normierte Polynom $P \in K[X]$ mit $P(f) = 0$, welches von minimalem Grad mit dieser Eigenschaft ist, das *Minimalpolynom* von f.

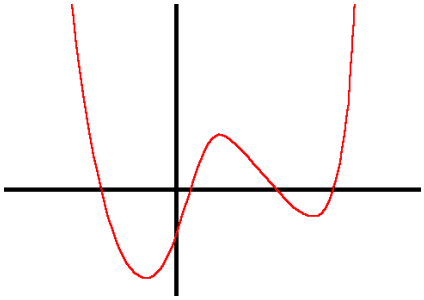
Galoiserweiterungen

Wir erwähnen hier ohne Beweis einige Hauptresultate über die Galoisgruppe und Galoiserweiterungen.

Definition 5.14. Es sei $K \subseteq L$ eine Körpererweiterung. Dann nennt man die Automorphismengruppe

$$\mathrm{Gal}\,(L|K) = \mathrm{Aut}_K\,(L)$$

die *Galoisgruppe* der Körpererweiterung.



Unter einem K-Körperautomorphismus φ muss ein Element $x \in L$, dass Nullstelle eines Polynoms F aus $K[X]$ ist, auf eine Nullstelle dieses Polynoms abgebildet werden. Das schränkt die Möglichkeiten wesentlich ein.

Es ist eine grundlegende Frage, welche Eigenschaften eines Elementes $x \in L$ unter einem K-Algebraautomorphismus erhalten bleiben und welche nicht.

LEMMA 5.15. *Es sei $K \subseteq L$ eine Körpererweiterung, $x \in L$, $F \in K[X]$ ein Polynom mit $F(x) = 0$ und sei $\varphi \in \operatorname{Gal}(L|K)$. Dann ist auch $F(\varphi(x)) = 0$.*

SATZ 5.16. *Es sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist die Galoisgruppe $\operatorname{Gal}(L|K)$ endlich.*

Aus dem Lemma von Dedekind ergibt sich eine direkte Abschätzung zwischen der Ordnung der Galoisgruppe und dem Grad einer endlichen Körpererweiterung.

SATZ 5.17. *Es sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist*

$$\#\left(\operatorname{Gal}(L|K)\right) \leq \operatorname{grad}_K L.$$

Eine wichtige Frage ist, wann in der vorstehenden Abschätzung Gleichheit vorliegt, wann es also so viele Automorphismen wie möglich gibt. Dies machen wir zur Grundlage der folgenden Definition. Es gibt eine Vielzahl an dazu äquivalenten Eigenschaften.

DEFINITION 5.18. Es sei $K \subseteq L$ eine endliche Körpererweiterung. Sie heißt eine *Galoiserweiterung*, wenn

$$\#\left(\operatorname{Gal}(L|K)\right) = \operatorname{grad}_K L$$

gilt.

Endliche Körper

Wir erwähnen eine wichtige Besonderheit für Ringe in positiver Charakteristik.

Definition 5.19. Es sei R ein kommutativer Ring, der einen Körper der positiven Charakteristik $p > 0$ enthalte. Der *Frobeniushomomorphismus* ist der Ringhomomorphismus

$$R \longrightarrow R,\, f \longmapsto f^p.$$

Wir fassen die wichtigsten Resultate über endliche Körper ohne Beweise zusammen. Für Beweise siehe den Kurs über Galoistheorie.

Satz 5.20. *Es sei p eine Primzahl und $e \in \mathbb{N}_+$. Dann gibt es bis auf Isomorphie genau einen Körper mit $q = p^e$ Elementen.*

Notation 5.21. Sei p eine Primzahl und $e \in \mathbb{N}_+$. Der aufgrund von Satz 5.20 bis auf Isomorphie eindeutig bestimmte endliche Körper mit $q = p^e$ Elementen wird mit

$$\mathbb{F}_q$$

bezeichnet.

Lemma 5.22. *Es sei L ein endlicher Körper der Charakteristik p. Dann ist der Frobeniushomomorphismus*

$$\Phi\colon\, L \longrightarrow L,\, x \longmapsto x^p,$$

ein Automorphismus, dessen Fixkörper $\mathbb{Z}/(p)$ ist.

Satz 5.23. *Es sei p eine Primzahl und $m \in \mathbb{N}$, $q = p^m$. Dann ist die Körpererweiterung $\mathbb{F}_p \subseteq \mathbb{F}_q$ eine Galoiserweiterung mit einer zyklischen Galoisgruppe der Ordnung m, die vom Frobeniushomomorphismus erzeugt wird.*

Abbildungsverzeichnis