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

# Algebraische Zahlentheorie

## Vorlesung 3

Wir haben in der letzten Vorlesung gesehen, dass sowohl die ganzen Zahlen $\mathbb{Z}$ als auch die Polynomringe $K[X]$ in einer Variablen über einem Körper $K$ Hauptidealbereiche sind. Bei Polynomen denkt man direkt an Funktionen, Auswertung an einem Punkt, Nullstellen, Ableitung u.s.w. Wir werden im Verlaufe dieser Vorlesung sehen, dass diese Konzepte zu einem Großteil auch im zahlentheoretischen Kontext interpretierbar sind.

## Zahlen und Funktionen

Zwischen den ganzen Zahlen einerseits und den Polynomringen über einem Körper andererseits bestehen folgende Analogien, die wir hier schon mal festhalten und die wir im Laufe des Kurses vertiefen werden. Dabei haben diese Phänomene im funktionentheoretischen Kontext eine zumeist naheliegende Bedeutung, während sie im zahlentheoretischen Kontext erst erschlossen werden müssen. Dieser Prozess erlaubt es, eine geometrische Sprache in die Zahlentheorie einzuführen, die zu Beginn etwas gewöhnungsbedürftig ist, aber bald eine gute intuitive Unterstützung für das Verständnis der Zahlentheorie gibt. Wir erwähnen die folgenden Punkte, die wir hier nur kurz funktionentheoretisch erläutern. Mit der passenden Begrifflichkeit werden aus Analogien dann gemeinsame Konzepte.

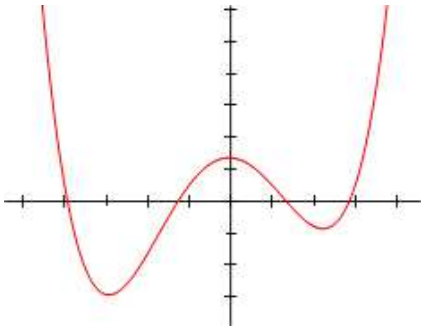
Analogien

(1) Man kann die gleichen algebraischen Konzepte anwenden.
(2) Hauptidealbereich.
(3) Punktkonzept. Restekörper.
(4) Funktion. Nullstelle.
(5) Rationale Funktionen. Polstelle.
(6) Quotientenkörper.
(7) Bilder und Urbilder.
(8) Lokale und globale Eigenschaften.
(9) Erweiterungen der Quotientenkörper. Ganzheit.
(10) Gruppenoperation.
(11) Zerlegung.
(12) Verzweigung.
(13) Singularitäten.
(14) Projektiver Abschluss.

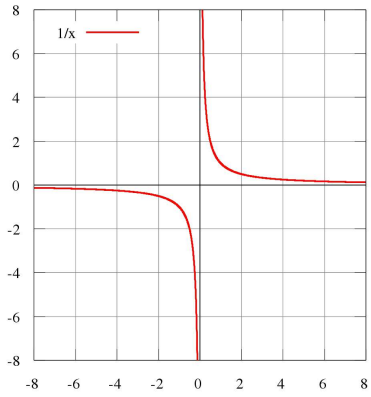
Unterschiede

(1) Nichtidentische Ringhomomorphismen von $K[T]$ in sich.
(2) Endlichkeit der Restekörper bei $\mathbb{Z}$. Dies gilt auch, wenn $K$ ein endlicher Körper ist. Diese „Enge“ erzwingt häufig zusätzliche Gesetzmäßigkeiten.
(3) Analytische Methoden bei $K = \mathbb{R}$ oder $K = \mathbb{C}$.
(4) Topologische Methoden bei $K = \mathbb{R}$ oder $K = \mathbb{C}$.

Einige Kommentare



Ein Polynom hat an jedem Punkt $a \in K$ einen Wert, eine besondere Rolle spielen die Nullstellen. Die Nullstellen können, wie bei $x^2$, eine größere Vielfachheit haben, und dies ist dann der Fall, wenn auch noch die Ableitung eine Nullstelle an dieser Stelle besitzt. Es gibt stets, außer beim Nullpolynom, nur endlich viele Nullstellen. Auch sonst wird jeder Wert, außer bei konstanten Polynomen, nur endlich oft angenommen. Über den komplexen Zahlen ist jedes nichtkonstante Polynom surjektiv.




Die rationale Funktion $1/x$ besitzt an der Stelle 0 einen Pol.

Aus Polynomen kann man durch Division auch rationale Funktionen bilden, beispielsweise $1/x$, diese sind nicht überall definiert und haben an endlich vielen Stellen, nämlich den Nullstellen des Nenners, Pole. Die Menge der rationalen Funktionen bildet wie die Menge der rationalen Zahlen einen Körper.

So wie man endliche Erweiterungen

$$\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{7}] = \mathbb{Z}[T]/(T^2-7)$$

betrachten kann, kann man auch Erweiterungen wie

$$K[Y] \subseteq K[Y][X]/(X^2-Y^3+5Y-4)$$

betrachten, dabei wird beispielsweise einem Polynom, hier $Y^3-5Y+4$, eine algebraische Quadratwurzel verpasst. Es wird also eine algebraische Funktion $\sqrt{y^3-5y+4}$ adjungiert. Eine Besonderheit tritt auf, wenn man aus der Variablen $Y$ selbst die Quadratwurzel zieht. Dann ist nämlich

$$K[Y][X]/(X^2-Y) \cong K[X],$$

da man ja $Y$ als Polynom in $X$ ausdrücken kann. In diesem Fall ist also der algebraisch definierte Erweiterungsring selbst wieder isomorph zum Polynomring selbst! Jedes Polynom $P(X)$ in einer Variablen kann man in diesem Sinne als Ringerweiterung

$$K[Y] \subseteq K[Y,X]/(Y-P(X)) \cong K[X]$$

interpretieren. Das Polynom $P$ definiert in diesem Sinne einen Ringhomomorphismus von $K[Y]$ nach $K[X]$. Ferner ist die Menge

$$V(Y-P(X)) = \left\{(x,y) \in K^2 \mid y = P(x)\right\}$$

der Graph des Polynoms $P$. Die Abbildung

$$K \longrightarrow K,\, x \longmapsto P(x),$$

kann man darin auch so auffassen, dass zuerst eine Bijektion zwischen $K$ und dem Graphen gemacht wird und dann der Graph auf die vertikale Achse projiziert wird. Bei dieser Interpretation sieht man besonders schön, welche Punkte auf einen bestimmten Punkt $b$ abgebildet werden, nämlich die Schnittpunkte des Graphen mit der durch $b$ verlaufenden horizontalen Geraden. Es ist im Hinblick auf die zahlentheoretische Interpretation üblich, das Bild an der Hauptdiagonalen zu spiegeln, dass der Graph oberhalb der Zielgeraden liegt und die Punkte quasi herunterfallen. Das Urbild von $b$ besteht bei dieser Veranschaulichung aus den Punkten, die oberhalb von $b$ liegen, und man interessiert sich insbesondere dafür, wie diese Fasern mit $b$ variieren. Bei einfachen Beispielen wie $P(x) = x^2$ fällt direkt ein regelmäßiges Zerlegungsverhalten der Fasern auf. Für reelles $b$ besteht bei $b$ positiv die Faser aus $\{\sqrt{b}, -\sqrt{b}\}$, bei $b = 0$ nur aus dem Nullpunkt und bei $b$ negativ ist die Faser leer. Im Komplexen besteht die Faser für $b \neq 0$ stets aus zwei Punkten. Die Einzigkeit der 0 über der 0 wird in einem gewissen Sinne dadurch „aufgefangen“, dass dort auch die Ableitung gleich 0 ist, dort fallen die beiden Urbilder zusammen, es liegt „Verzweigung“ vor.

Ein vergleichbares Verhalten zeigt sich bei der Ringerweiterung

$$\mathbb{Z} \subseteq \mathbb{Z}[\mathrm{i}],$$

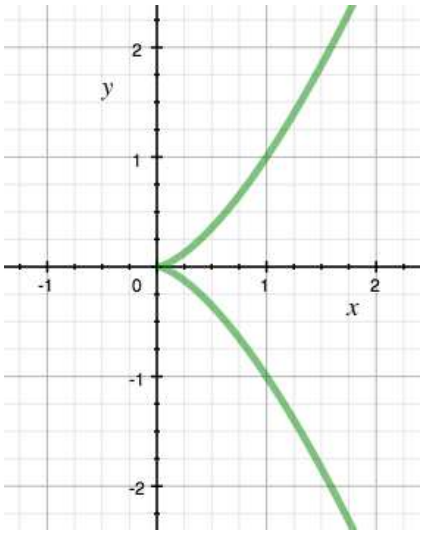
wenn man betrachtet, was dort mit den Primzahlen passiert. Für eine Primzahl $p$ mit dem Rest 1 modulo 4 gibt es dort (das haben wir in der ersten Vorlesung angedeutet und werden wir im Laufe es Kurses genauer begründen) eine Faktorzerlegung

$$p = x^2 + \mathrm{i}y^2 = (x + \mathrm{i}y)(x - \mathrm{i}y)$$

in zwei neue Primelemente, eine Primzahl $p$ mit dem Rest 3 modulo 4 bleibt eine Primzahl, wobei der Restklassenkörper aber $p^2$ viele Elemente besitzt, und für $p = 2$ gilt

$$2 = -\mathrm{i}(1 + \mathrm{i})^2,$$

was dem Verzweigungsverhalten entspricht.




Ein weiteres Phänomen tritt auf, wenn man Erweiterungen der Form

$$K[Y] \subseteq K[Y][X]/(X^2 - Y^3)$$

betrachtet, die zugehörige Kurve

$$V(X^2 - Y^3) = \left\{(x, y) \mid x^2 = y^3\right\}$$

besitzt eine Singularität im Punkt $(0, 0)$, was bei dem Graphen eines Polynoms nicht vorkommen kann. Zahlentheoretisch treten bei Erweiterungen wie $\mathbb{Z} \subseteq \mathbb{Z}[X]/(X^2 - 27)$, also der Adjunktion von $\sqrt{27}$, ähnliche Phänomene auf. Deshalb haben wir bei quadratischen Erweiterungen quadratfreie Zahlen gefordert, was wir im Rahmen der Ganzheitstheorie aber noch weiter vertiefen müssen.

## Primideale

Was ist ein Punkt? Im funktionentheoretischen Kontext, wenn es darum geht, Polynome in einer Variablen auszuwerten, ist ein Punkt einfach ein Element von $K$, sagen wir $a \in K$. Durch Einsetzen erhält man einen Ringhomomorphismus

$$K[X] \longrightarrow K,\ F \longmapsto F(a),$$

einem Polynom wird also der Wert an der Stelle $a$ zugeordnet. Diese Abbildung nennt man *Evaluation* $\mathrm{Ev}_a$ an der Stelle $a$. Ferner kennt man die Beziehung, dass $F(a) = 0$ genau dann ist, wenn $X - a$ im Polynomring ein Teiler von $F$ ist, siehe Lemma 19.8 (Lineare Algebra (Osnabrück 2017-2018)). Dies bedeutet, dass der Kern der Evaluationsabbildung das von der Linearform $X - a$ erzeugte Hauptideal ist. Über den komplexen Zahlen gilt ferner, dass $a_1, \ldots, a_k \in \mathbb{C}$ alle Nullstellen von $F$ sind, wenn für $F$ die Faktorzerlegung

$$F = (X - a_1)^{r_1} \cdots (X - a_k)^{r_k}$$

gilt. Die Punkte $a_i$ entsprechen also über die Linearformen $X - a_i$ den Primteilern von $F$. In einem gewissen Sinn entsprechen also Punkte speziellen Primelementen, in $\mathbb{C}[X]$ sind auch alle Primelemente von dieser linearen Form. Da nicht jeder Ring faktoriell ist, betrachtet man ausgehend vom Ring die sogenannten Primideale und entwickelt eine Theorie, in der diese Primideale zu Punkten eines geometrischen Objektes werden, und auf dem die Ringelemente zu Funktionen werden.

Definition 3.1. Ein Ideal $\mathfrak{p}$ in einem kommutativen Ring $R$ heißt *Primideal*, wenn $\mathfrak{p} \neq R$ ist und wenn für $r, s \in R$ mit $r \cdot s \in \mathfrak{p}$ folgt: $r \in \mathfrak{p}$ oder $s \in \mathfrak{p}$.

Lemma 3.2. *Es sei $R$ ein Integritätsbereich und $p \in R$, $p \neq 0$. Dann ist $p$ genau dann ein Primelement, wenn das von $p$ erzeugte Hauptideal $(p)$ ein Primideal ist.*

*Beweis.* Siehe Aufgabe 3.9. □

Lemma 3.3. *Es sei $R$ ein kommutativer Ring und $\mathfrak{p}$ ein Ideal in $R$. Dann ist $\mathfrak{p}$ genau dann ein Primideal, wenn der Restklassenring $R/\mathfrak{p}$ ein Integritätsbereich ist.*

*Beweis.* Sei zunächst $\mathfrak{p}$ ein Primideal. Dann ist insbesondere $\mathfrak{p} \subset R$ und somit ist der Restklassenring $R/\mathfrak{p}$ nicht der Nullring. Sei $fg = 0$ in $R/\mathfrak{p}$ wobei $f, g$ durch Elemente in $R$ repräsentiert seien. Dann ist $fg \in \mathfrak{p}$ und damit $f \in \mathfrak{p}$ oder $g \in \mathfrak{p}$. was in $R/\mathfrak{p}$ gerade $f = 0$ oder $g = 0$ bedeutet.

Ist umgekehrt $R/\mathfrak{p}$ ein Integritätsbereich, so handelt es sich nicht um den Nullring und daher ist $\mathfrak{p} \neq R$. Sei $f, g \notin \mathfrak{p}$. Dann ist $f, g \neq 0$ in $R/\mathfrak{p}$ und daher $fg \neq 0$ in $R/\mathfrak{p}$, also ist $fg \notin \mathfrak{p}$. □

Definition 3.4. Ein Ideal $\mathfrak{m}$ in einem kommutativen Ring $R$ heißt *maximales Ideal*, wenn $\mathfrak{m} \neq R$ ist und wenn es zwischen $\mathfrak{m}$ und $R$ keine weiteren Ideale gibt.

LEMMA 3.5. *Es sei $R$ ein kommutativer Ring und $\mathfrak{m}$ ein Ideal in $R$. Dann ist $\mathfrak{m}$ genau dann ein maximales Ideal, wenn der Restklassenring $R/\mathfrak{m}$ ein Körper ist.*

*Beweis.* Siehe Aufgabe 3.7. □

KOROLLAR 3.6. *Es sei $R$ ein kommutativer Ring und $\mathfrak{m}$ ein maximales Ideal in $R$. Dann ist $\mathfrak{m}$ ein Primideal.*

*Beweis.* Dies folgt sofort aus den Charakterisierungen für Primideale und für maximale Ideale mit den Restklassenringen. □

Zu einem Primideal $\mathfrak{p}$ und insbesondere zu einem maximalen Ideal gehört die *Evaluationsabbildung*

$$R \longrightarrow R/\mathfrak{p},$$

wobei im maximalen Fall rechts ein Körper steht, der *Restklassenkörper* oder *Restekörper* (bei einem Primideal betrachtet man den Quotientenkörper als Restekörper). Die Restklassenkörper sind für das Studium des Ringes relevante Körper. Bei $R = \mathbb{Z}$ sind die Evaluationsabildungen gleich $\mathbb{Z} \to \mathbb{Z}/(p)$ bzw. (zum Nullideal) $\mathbb{Z} \to \mathbb{Q}$. Hier treten also alle Primkörper als Restekörper auf.

LEMMA 3.7. *Es sei $R$ ein Hauptidealbereich und $p \neq 0$ ein Element. Dann sind folgende Bedingungen äquivalent.*

(1) *$p$ ist ein Primelement.*
(2) *$R/(p)$ ist ein Integritätsbereich.*
(3) *$R/(p)$ ist ein Körper.*

*Beweis.* Die Äquivalenz (1) $\Leftrightarrow$ (2) gilt in jedem kommutativen Ring (auch für $p = 0$), siehe Aufgabe 3.10, und (3) impliziert natürlich (2). Sei also (1) erfüllt und sei $a \in R/(p)$ von 0 verschieden. Wir bezeichnen einen Repräsentanten davon in $R$ ebenfalls mit $a$. Es ist dann $a \notin (p)$ und es ergibt sich eine echte Idealinklusion $(p) \subset (a, p)$. Ferner können wir $(a, p) = (b)$ schreiben, da wir in einem Hauptidealring sind. Es folgt $p = cb$. Da $c$ keine Einheit ist und $p$ prim (also nach Lemma 2.6 auch irreduzibel) ist, muss $b$ eine Einheit sein. Es ist also $(a, p) = (1)$, und das bedeutet modulo $p$, also in $R/(p)$, dass $a$ eine Einheit ist. Also ist $R/(p)$ ein Körper. □

In einem Hauptideal besteht also die Menge der Primideale aus dem Nullideal und den maximalen Idealen.

LEMMA 3.8. *Es sei $K$ ein Körper und $P \in K[X]$, $P \neq 0$, ein Polynom. Dann ist $P$ genau dann irreduzibel, wenn der Restklassenring $K[X]/(P)$ ein Körper ist.*

*Beweis.* Dies folgt direkt aus Satz 2.12 und Lemma 3.7. □

Wir erwähnen noch den folgenden Existenzsatz für Primideale.

LEMMA 3.9. *Es sei $R$ ein kommutativer Ring und sei $f \in R$ nicht nilpotent. Dann gibt es ein Primideal $\mathfrak{p}$ in $R$ mit $f \notin \mathfrak{p}$.*

*Beweis.* Siehe Aufgabe 3.8. □

## Das Spektrum

DEFINITION 3.10. Zu einem kommutativen Ring $R$ nennt man die Menge der Primideale von $R$ das *Spektrum* von $R$, geschrieben

$$\operatorname{Spek}(R).$$

BEISPIEL 3.11. Ein Körper hat bekanntlich nur zwei Ideale, nämlich das Einheitsideal $K$, das kein Primideal ist, und das Nullideal 0, das ein Primideal ist. Das Spektrum eines Körpers besteht also aus einem einzigen Punkt.

Bei einem Hauptidealbereich (dies gilt auch für Dedekindbereiche, die wir später einführen werden) besteht das Spektrum aus dem Nullideal 0 und den maximalen Idealen, die von der Form $\mathfrak{m} = (p)$ mit einem Primelement $p$ sind.

DEFINITION 3.12. Auf dem Spektrum eines kommutativen Ringes $R$ ist die *Zariski-Topologie* dadurch gegeben, dass zu einer beliebigen Teilmenge $T \subseteq R$ die Mengen

$$D(T) := \{\mathfrak{p} \in \operatorname{Spec}(R) \mid T \not\subseteq \mathfrak{p}\}$$

als offen erklärt werden.

Für einelementige Teilmengen $T = \{f\}$ schreiben wir $D(f)$ statt $D(\{f\})$.

LEMMA 3.13. *Die Zariski-Topologie auf dem Spektrum* $\operatorname{Spek}(R)$ *eines kommutativen Ringes $R$ ist in der Tat eine Topologie.*

*Beweis.* Siehe Aufgabe 3.16. □

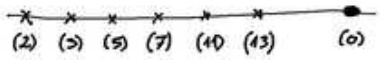
Wir betrachten das Spektrum stets als topologischen Raum. Die Primideale sind die Punkte dieses Raumes. Die Komplemente der offenen Mengen, also die abgeschlossenen Mengen in der Zariski-Topologie, werden mit

$$V(T) = \{\mathfrak{p} \in \operatorname{Spek}(R) \mid T \subseteq \mathfrak{p}\}$$

bezeichnet. Bei einem Hauptidealbereich ist die Zariski-Topologie besonders einfach, nur das gesamte Spektrum ist abgeschlossen und jede endliche Ansammlung von maximalen Idealen ist abgeschlossen. Dennoch ist auch in diesem Fall die Zariski-Topologie schon hilfreich. Wenn man beispielsweise aus topologischen Gründen weiß, dass eine Teilmenge abgeschlossenen sein muss, so folgt, dass es die gesamte Menge oder aber, dass sie endlich ist.

Beispiel 3.14. Für den Polynomring $R = K[X]$ in einer Variablen $X$ über einem Körper $K$ gibt es das Nullideal und die maximalen Ideale. Zu jedem Element $a \in K$ gehört die Linearform $X - a$ und das davon erzeugte maximale Ideal $(X - a)$. Deshalb stellt man sich das Spektrum $\operatorname{Spek}(K[X])$ zunächst als eine $K$-Gerade vor, mit dem fetten Punkt zum Nullideal als alles umfassenden Punkt. Bei $K$ algebraisch abgeschlossen ist dies das gesamte Spektrum. Bei einem nicht algebraisch abgeschlossenen Körper kommt noch für jedes normierte irreduzible Polynom $P$ vom Grad $\geq 2$ das maximale Primideal $(P)$ hinzu, das man aber im Bild schlecht skizzieren kann und sich „im Hintergrund“ vorstellt.

Beispiel 3.15. Die Primideale in $\mathbb{Z}$ sind einerseits die maximalen Ideale $(p)$, wobei $p$ eine Primzahl ist, und andererseits das Nullideal 0. Die maximalen Ideale bilden die abgeschlossenen Punkte von $\operatorname{Spek}(\mathbb{Z})$. Das Nullideal ist darin ein weiterer nicht abgeschlossener Punkt. Die einzige abgeschlossene Menge, in der dieser Punkt enthalten ist, ist die ganze Menge. Die abgeschlossenen Mengen in $\operatorname{Spek}(\mathbb{Z})$ sind neben der Gesamtmenge die endlichen Teilmengen aus maximalen Idealen.




So stellt man sich das Spektrum von $\mathbb{Z}$ vor. Die Verbindungslinien sollen vermitteln, dass es sich um ein eindimensionales Objekt handelt. Das Nullideal malt man fett, um anzudeuten, dass es sich um einen dichten Punkt handelt.

Man visualisiert $\operatorname{Spek}(\mathbb{Z})$ als eine (gedachte Gerade), auf der die Primzahlen diskret liegen, während der Nullpunkt ein fetter Punkt ist, der die gesamte Gerade repräsentiert.

Proposition 3.16. *Für das Spektrum $X = \operatorname{Spek}(R)$ eines kommutativen Ringes $R$ gelten folgende Eigenschaften.*

(1) *Es ist $D(T) = D(\mathfrak{a})$, wobei $\mathfrak{a}$ das durch $T$ erzeugte Ideal (Radikal) in $R$ sei. Man kann sich also bei der Beschreibung der offenen Teilmengen auf die Radikale von $R$ beschränken.*
(2) *Für eine Familie $\mathfrak{a}_i$, $i \in I$, von Idealen in $R$ ist*

$$\bigcup_{i \in I} D(\mathfrak{a}_i) = D\left( \sum_{i \in I} \mathfrak{a}_i \right).$$

(3) *Für eine endliche Familie* $\mathfrak{a}_i$, $i = 1, \ldots, n$, *von Idealen in* $R$ *ist*

$$\bigcap_{i=1}^{n} D(\mathfrak{a}_i) = D\left(\bigcap_{i=1}^{n} \mathfrak{a}_i\right) = D(\mathfrak{a}_1 \cdots \mathfrak{a}_n).$$

(4) *Es ist* $D(\mathfrak{a}) = X$ *genau dann, wenn* $\mathfrak{a}$ *das Einheitsideal ist.*
(5) *Es ist* $D(\mathfrak{a}) \subseteq D(\mathfrak{b})$ *genau dann, wenn* $\mathfrak{a} \subseteq \operatorname{rad}(\mathfrak{b})$ *gilt.*
(6) *Das Spektrum ist genau dann leer, wenn* $R$ *der Nullring ist.*
(7) *Es ist* $D(\mathfrak{a}) = \emptyset$ *genau dann, wenn* $\mathfrak{a}$ *nur nilpotente Elemente enthält.*
(8) *Die offenen Mengen* $D(f)$, $f \in R$, *bilden eine Basis der Topologie.*
(9) *Eine Familie von offenen Mengen* $D(\mathfrak{a}_i)$, $i \in I$, *ist genau dann eine Überdeckung von* $X$, *wenn die Ideale* $\mathfrak{a}_i$ *zusammen das Einheitsideal erzeugen.*

*Beweis.* Siehe Aufgabe 3.17. □

# Abbildungsverzeichnis