Prof. Dr. H. Brenner **Osnabrück SS 2011**

Körper- und Galoistheorie

Vorlesung 3

Es sei $K \subseteq L$ eine endliche Körpererweiterung und $x \in L$ ein Element. Dann sind die Potenzen x^i, $i \in \mathbb{N}$, linear abhängig, und das bedeutet, dass es Koeffizienten $a_i \in K$ mit $a_n \neq 0$ gibt mit $a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = 0$. Mit diesen Koeffizienten können wir das (von 0 verschiedene) Polynom

$$P = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n \in K[X]$$

bilden. Wenn man in dieses Polynom x einsetzt, d.h. überall die Variable X durch x ersetzt, so ergibt sich 0. Das Ergebnis dieses Einsetzens bezeichnet man mit $P(x)$, es ist also $P(x) = 0$. Man sagt, dass P das Element x *annuliert*. Wir betrachten die Menge

$$I = \{P \in K[X] | \, P(x) = 0\} \subseteq K[X] \, ,$$

also die Menge aller Polynome, die bei Einsetzung von x zu 0 werden.[1] Es ergeben sich dabei folgende Fragen.

(1) Welche Struktur besitzt I?
(2) Gibt es unter den Elementen $P \in I$ besonders einfache Polynome, mit denen man I einfach beschreiben kann?
(3) Kann man mit I Eigenschaften von $x \in L$ beschreiben?

Zu all diesen Fragen gibt es überzeugende Antworten. Zur ersten Frage können wir folgende Beobachtung machen: Das Nullpolynom gehört zu I. Wenn zwei Polynome P_1, P_2 zu I gehören, so gehört auch ihre Summe zu I, es ist ja $(P_1 + P_2)(x) = P_1(x) + P_2(x) = 0 + 0 = 0$. Für $P \in I$ und ein beliebiges Polynom $F \in K[X]$ ist auch $FP \in I$, wegen $(FP)(x) = F(x) \cdot P(x) = F(x) \cdot 0 = 0$.

Ideale

Die soeben formulierten Eigenschaften der Menge von annulierenden Polynomen führt zur folgenden Definition.

Definition 3.1. Eine nichtleere Teilmenge $\mathfrak{a}$ eines kommutativen Ringes R heißt *Ideal*, wenn die beiden folgenden Bedingungen erfüllt sind:

(1) Für alle $a, b \in \mathfrak{a}$ ist auch $a + b \in \mathfrak{a}$.
(2) Für alle $a \in \mathfrak{a}$ und $r \in R$ ist auch $ra \in \mathfrak{a}$.

[1] In der letzten Vorlesung haben wir gesehen, dass eine Einheitswurzel ζ nach Definition von $X^n - 1$ annuliert wird, bei $\zeta \neq 1$ aber auch von $X^{n-1} + \ldots + X^1 + 1$. Gibt es noch weitere annulierende Polynome? Gibt es noch weitere annulierende Polynome von kleinerem Grad?

Ein Ideal ist eine Untergruppe der additiven Gruppe von R, die zusätzlich die zweite oben angeführte Eigenschaft erfüllt. Die einfachsten Ideale sind das *Nullideal* 0 und das *Einheitsideal* R.

Für den Ring der ganzen Zahlen $\mathbb{Z}$ sind Untergruppen und Ideale identische Begriffe. Dies folgt einerseits aus der Gestalt $H = \mathbb{Z}d$ für jede Untergruppe von $\mathbb{Z}$ (die ihrerseits aus der Division mit Rest) aber ebenso direkt aus der Tatsache, dass für $k \in H$ und beliebiges $r \in \mathbb{N}$ gilt $rk = k + k + \ldots + k$ (r-mal) und entsprechend für negatives r. Die Skalarmultiplikation mit einem beliebigen Ringelement lässt sich also bei $\mathbb{Z}$ auf die Addition zurückführen.

Definition 3.2. Ein Ideal $\mathfrak{a}$ in einem kommutativen Ring R der Form

$$\mathfrak{a} = (a) = Ra = \{ra : r \in R\}.$$

heißt *Hauptideal*.

Definition 3.3. Zu einer Familie von Elementen $a_j \in R$, $j \in J$, in einem kommutativen Ring R bezeichnet $(a_j : j \in J)$ das von den a_j *erzeugte Ideal*. Es besteht aus allen (endlichen) *Linearkombinationen*

$$\sum_{j \in J_0} r_j a_j \,,$$

wobei $J_0 \subseteq J$ eine endliche Teilmenge und $r_j \in R$ ist.

Es handelt sich dabei um das kleinste Ideal in R, das alle a_j, $j \in J$, enthält. Dass ein solches Ideal existiert ist auch deshalb klar, weil der Durchschnitt von einer beliebigen Familie von Idealen wieder ein Ideal ist. Ein Hauptideal ist demnach ein Ideal, das von einem Element erzeugt wird.

Einige ringtheoretische Konzepte

In einem Körper folgt aus $xy = 0$, dass ein Faktor 0 sein muss. Diese Eigenschaft gilt nicht für beliebige Ringe. Ein Element $f \in R$ in einem kommutativen Ring heißt *Nichtnullteiler*, wenn aus $fg = 0$ stets $g = 0$ folgt. Man nennt einen Ring *nullteilerfrei*, wenn 0 der einzige Nullteiler ist.

Definition 3.4. Ein kommutativer, nullteilerfreier, von null verschiedener Ring heißt *Integritätsbereich*.

Der Ring $\mathbb{Z}$ der ganzen Zahlen und die Polynomringe $K[X]$ über einem Körper K sind Integritätsbereiche. Das sind für uns die wichtigsten Beispiele.

Definition 3.5. Ein Element u in einem kommutativen Ring R heißt *Einheit*, wenn es ein Element $v \in R$ mit $uv = 1$ gibt.

Definition 3.6. Sei R ein kommutativer Ring, und a, b Elemente in R. Man sagt, dass a das Element b *teilt* (oder dass b von a geteilt wird, oder dass b ein *Vielfaches* von a ist), wenn es ein $c \in R$ gibt derart, dass $b = c \cdot a$ ist. Man schreibt dafür auch $a|b$.

Definition 3.7. Sei R ein kommutativer Ring. Man sagt, dass zwei Elemente $a, b \in R$ *teilerfremd* sind, wenn jedes Element $c \in R$, das sowohl a als auch b teilt, eine Einheit ist.

Definition 3.8. Eine Nichteinheit p in einem kommutativen Ring heißt *irreduzibel* (oder *unzerlegbar*), wenn eine Faktorisierung $p = ab$ nur dann möglich ist, wenn einer der Faktoren eine Einheit ist.

Diese Begriffsbildung orientiert sich offenbar an den Primzahlen. Dagegen taucht das Wort „prim“ in der folgenden Definition auf.

Definition 3.9. Eine Nichteinheit $p \neq 0$ in einem kommutativen Ring R heißt *prim* (oder ein *Primelement*), wenn folgendes gilt: Teilt p ein Produkt ab mit $a, b \in R$, so teilt es einen der Faktoren.

Eine Einheit ist also nach Definition nie ein Primelement. Dies ist eine Verallgemeinerung des Standpunktes, dass 1 keine Primzahl ist. Dabei ist die 1 nicht deshalb keine Primzahl, weil sie „zu schlecht“ ist, sondern weil sie „zu gut“ ist. Für die ganzen Zahlen und für viele weitere Ringe fallen die beiden Begriffe prim und irreduzibel zusammen. Im Allgemeinen ist irreduzibel einfacher nachzuweisen, und prim ist der stärkere Begriff, jedenfalls für Integritätsbereiche.

Lemma 3.10. *In einem Integritätsbereich ist ein Primelement stets irreduzibel.*

Beweis. Angenommen, wir haben eine Zerlegung $p = ab$. Wegen der Primeigenschaft teilt p einen Faktor, sagen wir $a = ps$. Dann ist $p = psb$ bzw. $p(1 - sb) = 0$. Da p kein Nullteiler ist, folgt $1 = sb$, so dass also b eine Einheit ist. □

Irreduzible Polynome

Beispiel 3.11. Ein nichtkonstantes Polynom $P = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n \in K[X]$, wobei K einen Körper bezeichne, ist genau dann irreduzibel, wenn es keine Produktdarstellung

$$P = QR$$

gibt, die die Gradbedingung

$$0 < \deg(Q) < \deg(P)$$

erfüllt.

Die irreduziblen Polynome sind gerade die irreduziblen Elemente im Polynomring $K[X]$ im Sinne der obigen allgemeinen ringtheoretischen Definition.

Nach der weiter unten zu beweisenden Aussage könnte man auch von Primelementen bzw. Primpolynomen sprechen. Eine weitere wichtige Charakterisierung ist die Restklassencharakterisierung, die wir in der siebten Vorlesung kennenlernen werden.

Beispiel 3.12. Die Irreduzibilität eines Polynoms hängt wesentlich vom Grundkörper ab. Zum Beispiel ist das reelle Polynom $X^2+1 \in \mathbb{R}[X]$ irreduzibel, dagegen zerfällt es als Polynom in $\mathbb{C}[X]$ als

$$X^2+1 = (X+i)(X-i)\,.$$

Ebenso ist das Polynom $X^2-5 \in \mathbb{Q}[X]$ irreduzibel, aber über $\mathbb{R}$ hat es die Zerlegung

$$X^2-5 = (X-\sqrt{5})(X+\sqrt{5})\,.$$

Übrigens kann die Zerlegung über einem größeren Körper manchmal dazu benutzt werden um zu zeigen, dass ein Polynom über dem gegebenen Körper irreduzibel ist.

Die Existenz der Faktorzerlegung in der folgenden Aussage folgt unmittelbar aus der Definition von irreduzibel, für die Eindeutigkeit muss man aber wissen, dass in einem Polynomring die irreduziblen Polynome auch Primpolynome sind (siehe unten).

Satz 3.13. *Es sei K ein Körper und sei $F \in K[X]$ ein von 0 verschiedenes Polynom. Dann gibt es eine (bis auf die Reihenfolge der Faktoren) eindeutige Produktdarstellung*

$$F = aF_1 \cdots F_r$$

mit $a \in K^\times$ und irreduziblen normierten Polynomen F_i, $i = 1, \ldots, r$.

Beweis. Siehe Aufgabe 3.8. □

Hauptidealbereiche

Definition 3.14. Ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealbereich*.

Satz 3.15. *Ein Polynomring über einem Körper ist ein Hauptidealbereich.*

Beweis. Sei I ein von null verschiedenes Ideal in $K[X]$. Betrachte die nichtleere Menge

$$\{\operatorname{grad}(P) |\, P \in I,\, P \neq 0\}\,.$$

Diese Menge hat ein Minimum $m \in \mathbb{N}$, das von einem Element $F \in I$, $F \neq 0$, herrührt, sagen wir $m = \operatorname{grad}(F)$. Wir behaupten, dass $I = (F)$ ist. Sei hierzu $P \in I$ gegeben. Aufgrund von Satz Anhang 1.3 gilt

$$P = FQ + R \text{ mit } \operatorname{grad}(R) < \operatorname{grad}(F) \text{ oder } R = 0\,.$$

Wegen $R \in I$ und der Minimalität von $\operatorname{grad}(F)$ kann der erste Fall nicht eintreten. Also ist $R = 0$ und P ist ein Vielfaches von F. □

In der eingangs besprochenen Situation eines Elements $x \in L$ einer Körpererweiterung $K \subseteq L$ und des zugehörigen Annullationsideals

$$I = \{P \in K[X] | \, P(x) = 0\}$$

bedeutet dieser Satz, dass es ein Polynom geben muss, dass dieses Ideal erzeugt. Dieses Polynom besitzt unter sämtlichen annullierenden Polynomen $\neq 0$ minimalen Grad, und man kann es als normiert ansetzen, wodurch es eindeutig festgelegt wird. Man spricht vom *Minimalpolynom* zu x.

Mit einem ähnlichen Argument wie im Beweis der letzten Aussage verwendet kann man zeigen, dass $\mathbb{Z}$ ebenfalls ein Hauptidealbereich ist. Die folgenden Aussagen gelten also auch für $\mathbb{Z}$.

Die beiden folgenden Aussagen nennt man *Lemma von Bezout* bzw. *Lemma von Euklid*.

LEMMA 3.16. *Sei R ein Hauptidealbereich und seien $a, b \in R$ zwei teilerfremde Elemente. Dann kann man die 1 als Linearkombination von a und b darstellen, d.h. es gibt Elemente $r, s \in R$ mit $ra + sb = 1$.*

Beweis. Wir betrachten das von a und b erzeugte Ideal $I = (a, b)$. Da R ein Hauptidealbereich ist, gibt es ein $c \in R$ mit $(a, b) = (c)$. Daher ist c ein Teiler von a und von b. Die Teilerfremdheit impliziert, dass c eine Einheit ist. Wegen $c \in (a, b)$ gibt es eine Darstellung $c = ua + vb$. Multiplikation mit c^{-1} ergibt die Darstellung der 1. □

LEMMA 3.17. *Sei R ein Hauptidealbereich und $a, b, c \in R$. Es seien a und b teilerfremd und a teile das Produkt bc. Dann teilt a den Faktor c.*

Beweis. Da a und b teilerfremd sind, gibt es nach dem Lemma von Bezout Elemente $r, s \in R$ mit $ra + sb = 1$. Die Voraussetzung, dass a das Produkt bc teilt, schreiben wir als $bc = da$. Damit gilt

$$c \;=\; c1 \;=\; c(ra + sb) \;=\; cra + csb \;=\; a(cr + ds),$$

was zeigt, dass c ein Vielfaches von a ist. □

KOROLLAR 3.18. *Sei R ein Hauptidealbereich. Dann ist ein Element genau dann prim, wenn es irreduzibel ist.*

Beweis. Ein Primelement in einem Integritätsbereich ist nach Lemma 3.10 stets irreduzibel. Sei also umgekehrt p irreduzibel, und nehmen wir an, dass p das Produkt ab teilt, sagen wir $pc = ab$. Nehmen wir an, dass a kein Vielfaches von p ist. Dann sind aber a und p teilerfremd, da eine echte Inklusionskette $(p) \subset (p, a) = (d) \subset R$ der Irreduzibilität von p widerspricht. Damit teilt p nach dem Lemma von Euklid den anderen Faktor b. □