Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

9.Vorlesung

29. Mai 2017

Proposition 9.1
Seien R, S integritätsbereiche, $R \subseteq S$ und $\alpha \in S$. Es gilt: α ist genau dann ganz über R, wenn es einen endlich erzeugten R-Untermodul $M \neq 0$ von S gibt, so daß $\alpha M \subseteq M$.
(In der Tat können wir $M = R[\alpha]$ nehmen).

Beweis. „$\Rightarrow$“ Sei $\alpha^n + r_1\alpha^{n-1} + \cdots + r_n = 0$, $r_i \in R$.

Behauptung: $\mathrm{Span}_R\{1, \alpha, \ldots, \alpha^{n-1}\} := M$ hat die gewünschte Eigenschaft.

Beweis. $\alpha^n \in \sum_{i=0}^{n-1} R\alpha^i$, also ist
$\alpha(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = \alpha a_0 + a_1\alpha^2 + \cdots + a_{n-2}\alpha^{n-1} + a_{n-1} \underbrace{\alpha^n}_{\in \sum R\alpha^i}$

□

„$\Leftarrow$“

Erinnerung (Cramer's Formel)**:** Seien $d_1, \ldots, d_n \in R$, C eine $n \times n$ Matrix mit Einträgen in R, $C = (c_{ij})$, und sei C_j die Matrix, die man bekommt, nachdem wir die j-te Spalte von C durch $\begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}$ ersetzen. Sei $X := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ eine Lösung für
$CX = \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}$
Es gilt: $\det(C)x_j = \det(C_j) \forall j$

Sei nun $M \neq 0$ endlich erzeugt mit $\alpha M \subseteq M$ und $v_1, \ldots, v_n \in S$ Erzeuger für M. Für alle i gilt $\alpha v_i = \sum a_{ij}v_j$ für $a_{ij} \in R$. Umschreiben ergibt ein Gleichungssytem:

$$\begin{aligned} (\alpha - a_{11})v_1 - a_{12}v_2 - \cdots &= 0 \\ -a_{21}v_1 + (\alpha - a_{22})v_2 - \cdots &= 0 \\ &\vdots \\ \cdots &= 0 \end{aligned}$$

Sei C die Koeffizienten-Matrix. Cramers Formel ergibt für $C\underline{v} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$:

$\det(C)v_j = \det(C_j) = 0$
Da es mindestens ein j gibt mit $v_j \neq 0$ (weil $0 \neq M$), $v_j \in S$ und $\det(C) \in S$ und S integritätsbereich$\Rightarrow \det(C) = 0$.

Das Berechnen dieser Determinante ergibt schliesslich eine Gleichung
$\alpha^n + c\alpha^{n-1} + \cdots + c_n = 0$ (ÜA).

□

Notation
$\overline{R}^S := \{\alpha \in S \mid \alpha \text{ ist ganz über } R\}$.

Proposition 9.2
Seien $R \subseteq S$ Erweiterung von Integritätsbereichen. Der ganze Abschluß $\overline{R}^S$ von R in S ist ein Unterring von S.

Beweis. Seien $\alpha, \beta \in S$ ganz über R, $0 \neq M$, $0 \neq N$ endlich erzeugte R-Untermoduln von S, so daß $\alpha M \subseteq M$ und $\beta N \subseteq N$. Definiere $MN := \{\sum m_i n_i \mid m_i \in M, n_i \in N\}$.
Es ist:

(a) $MN \neq 0$ ist R-Untermodul von S

(b) MN ist endlich erzeugt (wenn $\{e_1, \ldots, e_m\}$ M erzeugt und $\{f_1, \ldots, f_n\}$ N erzeugt, dann erzeugt $\{e_i f_j \mid i = 1, \ldots, m, j = 1, \ldots, n\}$ MN).

(c) MN ist abgeschlossen unter multiplikation durch $\alpha\beta$ und $\alpha \pm \beta$ (d.h $\alpha\beta MN \subseteq MN$ und $(\alpha \pm \beta)MN \subseteq MN$, (ÜA)).

Anwendung von Proposition 9.1 ergibt: $\alpha\beta$ und $\alpha \pm \beta$ sind ganz über R. □

Korollar 9.3
Seien $R \subseteq S$ Integritätsbereiche. Es gilt: S endlich erzeugt als R-Modul$\Rightarrow$ S ist ganz über R.

Satz 9.4
Sei R ein Integritätsbereich, $K := \mathrm{Quot}(R)$, L/K eine algebraische Körpererweiterung und $\overline{R}^L$ der ganze Abschluß von R in L. Es gilt: $L = \mathrm{Quot}(\overline{R}^L)$.

Für den Beweis brauchen wir eine:

Proposition 9.5
Sei R ein Integritätsbereich, $K := \mathrm{Quot}(R)$,L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Dann gibt es $d \in R$ mit $d\alpha$ ganz über R.

Beweis. α erfüllt

$$(*) \qquad \alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$$

mit $a_i \in K = \mathrm{Quot}(R)$. Sei $d \in R$, so daß $\forall i, da_i \in R$. Multiplizieren von $(*)$ mit d^m ergibt $d^m\alpha^m + a_1 d^m \alpha^{m-1} + \cdots + a_m d^m = 0$, d.h $(d\alpha)^m + (a_1 d)(d\alpha)^{m-1} + \cdots + a_m d^m = 0$ □

Beweis vom Satz 9.4. $\alpha \in L$ lässt sich schreiben als $\alpha = \frac{d\alpha}{d}$, $d \in R, d\alpha \in \overline{R}^L$, d.h $\alpha \in \mathrm{Quot}(\bar{R}^L)$, also $\mathrm{Quot}(\bar{R}^L) \supseteq L$. Da die Inklusion $\mathrm{Quot}(\bar{R}^L) \subseteq L$ offensichtlich ist, ist der Satz bewiesen. □

§Ganz abgeschlossene Integritätsbereiche

Definition 9.1
Ein Integritätsbereich R ist ganz abgeschlossen $\Leftrightarrow$ $\overline{R}^K = R$, wobei $K := \mathrm{Quot}(R)$

Beispiel 9.1
Faktorielle Integritätsbereiche sind ganz abgeschlossen (ÜB)

Wir hatten gezeigt: R faktoriell, L/K Körpererweiterung, $\alpha \in L$ algebraisch über K, dann ist α ganz über $R \Leftrightarrow \mathrm{MinPol}_K(\alpha) \in R[x]$.
Wir verallgemeinern nun dieses:

Proposition 9.6
Sei R ein Integritätsbereich, $K = \mathrm{Quot}(R)$ und L/K eine algebraische Körpererweiterung. Wir nehmen an, daß R ganz abgeschlossen ist. Es gilt : $\alpha \in L$ ist ganz über $R \Leftrightarrow \mathrm{MinPol}_K(\alpha) \in R[x]$

Beweis. „$\Leftarrow$“:✓
„$\Rightarrow$“: Sei $\alpha \in L$ und $a_i \in R$, so daß

$$(*) \qquad \alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$$

Setze $f(x) = \mathrm{MinPol}_K(\alpha) \in K[x]$. Wir arbeiten in einem Zerfällungskörper für f und behaupten: alle Nullstellen von $f(x)$ sind ganz über R

Beweis. Sei α' eine Nullstelle, dann gilt
$K(\alpha) \underset{\sim}{\xrightarrow{\sigma}} K(\alpha')$ mit $\sigma_{|K} = \mathrm{Id}$ und $\alpha \mapsto \alpha'$
anwenden von σ auf $(*)$ ergibt
$(\alpha')^m + a_1(\alpha')^{m-1} + \cdots + a_m = 0$

□

Es folgt, daß alle Koeffizienten von $f(x)$ (diese Koeffizienten von $f(x)$ sind ja elementare symmetrische Polynome in den Nullstellen von $f(x)$) sind ganz über R (da die Menge aller ganzen Elementen ein Teilring ist). Diese Koeffiziente sind andererseits in $K = \mathrm{Quot}(R)$, also R ganz abgeschlossen $\Rightarrow$ alle Koeffiziente sind $\in R$. □

10