Algebraische Zahlentheorie

SS 2013

Kuhlmann

9. Vorlesung am 16.05.2013.

Proposition 1. Seien R, S Integritätsbereiche; $R \subseteq S$ und $\alpha \in R$.

Es gilt: α ist ganz über $R \iff$ es gibt einen endl. erz. R-Untermodul $0 \neq M$ von S so daß $\alpha M \subseteq M$.

(in der Tat können wir $M = R[\alpha]$ nehmen).

Beweis. "$\Rightarrow$" Sei $\alpha^n + r_1 \alpha^{n-1} + \dots + r_n = 0$

$r_i \in R$. Beh: $\operatorname{Span}_R \{1, \alpha, \dots, \alpha^{n-1}\} := M$

hat die gewünschte Eigenschaft.

Bew: $\alpha^n \in \sum_{i=0}^{n-1} R\alpha^i$ so

$$\alpha(a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}) =$$

$$\alpha a_0 + a_1\alpha^2 + \dots + a_{n-2}\alpha^{n-1} + a_{n-1}\underbrace{\alpha^n}_{\in \sum R\alpha^i}.$$ ∎

"$\Leftarrow$" ⌈ Erinnerung: Cramer's Formel

Sei R ein Ring   10. Vor LA II 18.05.2012

Seien $d_1, \dots, d_n \in R$, C eine $n \times n$ Matrix mit Einträgen in R

Schreibe $C = (c_{ij})$ und sei C_j die Matrix die man

bekommt nachdem wir die j^{te} Spalte von C durch $\begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}$;

$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ Lösung für $CX = \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}$

Es gelt:

$$\det C \; x_j = \det C_j \quad \forall j. \rfloor$$

Sei nun $0 \neq M$ endl. erz. mit $\alpha M \subseteq M$

und $v_1, \dots, v_n \in S$ Erzeuger für M.

$\forall i$ gelt $\alpha v_i = \sum a_{ij} v_j$ für $a_{ij} \in R$

Umschreiben ergibt ein Gleichungssystem

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

Sei C die Koeffizienten Matrix,

Cramer's Formel ergebt 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 $\Longrightarrow$ $\det(C) = 0$.

Das Berechnen dieser Determinante ergibt

schließlich eine Gleichung

(ÜA) $\alpha^n + c\alpha^{n-1} + \dots + c_n = 0$, $c_i \in R$. ■

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

__Proposition 2__ Seien $R \subseteq S$ Erweiterung von Integritätsber. Der ganze Abschluß $\overline{R}^S$ von R in S ist ein **Unterring** von S.

__Beweis.__ Seien $\alpha, \beta \in S$ ganz über R,

$0 \neq M$, $0 \neq N$ endl. erz. R- Untermoduln

von S s.d. $\alpha M \subseteq M$ 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 endl. erz (e.g wenn $\{e_1, \dots, e_m\}$

M erzeugt und $\{f_1, \dots, f_n\}$ N erzeugt

dann erzeugt $\{e_i f_j \; ; \; i = 1, \dots, m, \; j = 1, \dots, n\}$

MN.)

(c) MN ist abgeschloßen unter

multiplikation durch $\alpha\beta$ und $\alpha \pm \beta$;

(i.e $\alpha\beta \, MN \subseteq MN$ und $(\alpha \pm \beta) \, MN \subseteq MN$,

ü A).

Anwendung nun von Proposition 1 ergebt

$\alpha\beta$ und $\alpha \pm \beta$ sind ganz über R. ∎

<u>**Korollar 3**</u> Seien $R \subset S$ Integritätsbereiche.

Es gilt: S endl. erz. als R-Modul $\Rightarrow$
S ist ganz über R. ∎

<u>**Satz 4**</u>: Sei R Integritätsbereich
$K := \mathrm{Quot}(R)$
$L \mid K$ algebraische Körpererw.,
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 5. Sei R Integritätsbereich
$K := \mathrm{Quot}(R)$
$L \supseteq K$ Körpererw.,
und $\alpha \in L$ alg. über K.
Dann gibt es $d \in R$ mit $d\alpha$ ganz über R.

Beweis α erfüllt

$$(*) \qquad \alpha^m + a_1 \alpha^{m-1} + \dots + a_m = 0 \qquad a_i \in K = \mathrm{Quot}(R)$$

Sei $d \in R$ so daß $d a_i \in R \quad \forall i$;

und multiplizieren von $(*)$ mit d^m ergibt

$$d^m \alpha^m + a_1 d^m \alpha^{m-1} + \dots + a_m d^m = 0;$$

i.e

$$(d\alpha)^m + (a_1 d)(d\alpha)^{m-1} + \dots + a_m d^m = 0. \qquad \square$$

Beweis vom Satz 4:

$\alpha \in L$ läßt sich schreiben als

$$\alpha = \frac{d\alpha}{d} \quad ; \; d \in R, \; d\alpha \in \bar{R}^L$$

i.e $\alpha \in \mathrm{Quot}(\bar{R}^L)$.

Also $\mathrm{Quot}(\bar{R}^L) \supseteq L$; da die Inklusion
$\mathrm{Quot}(\bar{R}^L) \subseteq L$ offensichtlich ist ist der Satz bewiesen.
$\square$

Ganzabgeschloßene Integritätsbereiche.

Definition Ein Integritätsbereich R ist ganz abgeschloßen $\Leftrightarrow$

$$\overline{R}^{K} = R \quad \text{wobei } K := \mathrm{Quot}(R).$$

Bsp. Faktorielle Integritätsbereiche sind ganz abgeschloßen (Auf 1.1 ÜB 1 B4).

Wir hatten gezeigt: R Faktoriell, L/K körpererw, $\alpha \in L$ alg $/K$; dann ist α ganz über $R \Leftrightarrow$

$$\mathrm{MinPol}_K(\alpha) \in R[x].$$

Wir verallgemeinern nun dieses.

Proposition 6. Sei R Integritätsbereich; $K := \mathrm{Quot}(R)$, L/K alg. Körpererw.
Wir nehmen an: R sei ganzabgeschlossen.
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

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

Setze $f(x) = \mathrm{Min\,Pol}_K\, \alpha \quad \in K[x]$

Wir arbeiten in einem Zerfällungskörper für f;

und behaupten: alle NS von $f(x)$ sind ganz über R:

<u>Bew:</u> Sei α' eine NS dann gilt

$$K(\alpha) \xrightarrow{\sigma} K(\alpha') \quad \text{mit } \sigma|_K = \mathrm{Id}$$

$$\text{und} \quad \alpha \longmapsto \alpha';$$

anwenden von σ auf ⊛ ergibt

$$(\alpha')^m + a_1 (\alpha')^{m-1} + \dots + a_m = 0. \quad \square \text{ Beh.}$$

Es folgt daß alle Koeffizienten von $f(x)$

(diese Koeffizienten von $f(x)$ sind ja

elementare symmetrische Polynome in den NS 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 $\in R$. $\boxtimes$