UNTERLAGEN ZU POLYNOMEN UND KÖRPERN (ENTWURF)

VORLESUNG "ALGEBRA", SOMMERSEMESTER 2004

1. Definition von Körpern

Definition 1.1. *Eine Algebra* $\langle K, +, \cdot \rangle$ *ist ein* Körper*, wenn:*

(1) $\langle K, +, \cdot \rangle$ *ist ein kommutativer Ring.*
(2) $\langle K \setminus \{0\}, \cdot \rangle$ *ist eine Gruppe, wobei* 0 *das neutrale Element bezüglich* $+$ *ist.*

Definition 1.2. *Sei* $\langle E, +, \cdot \rangle$ *ein Körper. Ein Unterring* $\mathbf{K}$ *von* $\mathbf{E}$ *ist ein* Unterkörper *von* $\mathbf{E}$*, wenn* $\langle K, +, \cdot \rangle$ *ein Körper ist.*

Lemma 1.3. *Sei* $\mathbf{E}$ *ein Körper, und sei* K *eine Teilmenge von* E*. Dann ist* K *genau dann Trägermenge eines Unterkörpers von* $\mathbf{E}$*, wenn* $0_E \in K$*,* $1_E \in K$*, und für alle* $x, y \in K$ *auch* $x + y$*,* $x - y$*,* $x \cdot y$ *und* $x^{-1_{\mathbf{E}}}$ *in* K *liegen.*

Wenn $\mathbf{K}$ Unterkörper von $\mathbf{E}$ ist, so heißt $\mathbf{E}$ Körpererweiterung von $\mathbf{K}$.

2. Polynome

Definition 2.1. *Sei* $\mathbf{K}$ *kommutativer Ring mit Eins. Dann ist* $K[t] := \{a \in K^{\mathbb{N}_0} \mid \exists i \in \mathbb{N}\ \forall j \in \mathbb{N} : j \geq i \Rightarrow a_j = 0\}$*.*

Definition 2.2. *Addition und Multiplikation auf* $K[t]$*.*

Definition 2.3. *Sei* $f \in K[t]$*.* $\deg f := \ldots$, $\deg 0 := -1$.

Mit $t = (0, 1, 0, \ldots)$ gilt $a = (a_0, a_1, \ldots) = \sum_{i=0}^{\deg a} a_i t^i$.

Definition 2.4. *Sei* $\mathbf{K}$ *Körper, und seien* $f, g \in K[t]$*.*

(1) f *teilt* g*, wenn es* $q \in K[t]$ *gibt, sodass* $g = q \cdot f$*.*
(2) *Wenn* $f \neq 0$*, so gibt es* $q, r \in K[t]$ *mit* $g = q \cdot f + r$ *und* $\deg r < \deg f$*.*
(3) f *ist* invertierbar*, wenn* $\deg f = 0$*.*
(4) f *ist* irreduzibel über $\mathbf{K}$ *(ein irreduzibles Polynom in* $K[t]$*), wenn* $\deg f \geq 1$ *und für alle* $a, b \in K[t]$ *mit* $a \cdot b = f$ *entweder* a *oder* b *Grad* 0 *hat.*

Date: June 17, 2004.
Erhard Aichinger, Institut für Algebra, Johannes Kepler Universität Linz, Austria, erhard@algebra.uni-linz.ac.at.

(5) *f ist* normiert*, wenn es führenden Koeffizienten* 1 *hat.*

Definition 2.5. *Sei $\langle R, +, \cdot \rangle$ ein Ring, und sei $I \subseteq R$. I ist ein* Ideal *von* $\mathbf{R}$*, wenn für alle $i, j \in I$ und $r \in R$ gilt: $i - j \in I$, $r \cdot i \in I$, $i \cdot r \in I$.*

Kongruenzrelationen und Ideale eines Ringes sind einander durch $\alpha \mapsto 0/\alpha$ bijektiv zugeordnet.

Satz 2.6 ($\mathbf{K}[t]$ ist Hauptidealbereich)**.** *Sei $\mathbf{K}$ ein Körper, und sei I ein Ideal von $\mathbf{K}[t]$. Dann gibt es $f \in K[t]$ mit $I = \{p \cdot f \,|\, p \in K[t]\} = (f)$.*

Wenn $I \neq 0$, dann gilt für jedes f mit $\deg f = \min\{\deg i \,|\, i \in I \setminus \{0\}\}$, dass $I = (f)$.

Satz 2.7 (ggT in $\mathbf{K}[t]$)**.** *Sei $\mathbf{K}$ ein Körper, und seien $f, g \in K[t]$, nicht beide 0. Dann gibt es genau ein $d \in K[t]$, sodass*

(1) *$d|f$, $d|g$.*
(2) *Für alle u mit $u|f$ und $u|g$ gilt $u|d$.*
(3) *d ist normiert.*

Dieses d heißt der ggT *von f und g. Es gibt $u, v \in K[t]$, sodass $u \cdot f + v \cdot g = d$.*

Beweisskizze: Wir wählen für d einen normierten Erzeuger des Ideals $I = \{u \cdot f + v \cdot g \,|\, u, v \in K[t]\}$.

Satz 2.8. *Sei $\mathbf{K}$ Körper, $f \in K[t]$ irreduzibel über $\mathbf{K}$. Dann ist $\mathbf{K}[t]/(f)$ ein Körper.*

3. Zerfällungskörper

Satz 3.1. *Sei $\mathbf{K}$ ein Körper, und sei f ein normiertes Polynom in $\mathbf{K}[t]$ vom Grad n. Dann gibt es einen Erweiterungskörper $\mathbf{E}$ von $\mathbf{K}$, sodass jeder in $\mathbf{E}[t]$ irreduzible Teiler von f Grad 1 hat.*

Beweis: Wir beweisen folgende Aussage durch Induktion nach n:

> Für jeden Körper $\mathbf{K}$ und jedes normierte Polynom $f \in \mathbf{K}[t]$ vom Grad n gibt es einen Erweiterungskörper $\mathbf{E}$ von $\mathbf{K}$, sodass jeder in $\mathbf{E}[t]$ irreduzible Teiler von f Grad 1 hat.

Für $n = 1$ ist die Aussage klar. Wir fixieren nun einen Körper $\mathbf{K}$ und ein Polynom $f \in \mathbf{K}[t]$ mit $\deg f = n > 1$. Wir zerlegen f in ein Produkt von normierten, über $\mathbf{K}$ irreduziblen Polynomen in $\mathbf{K}[t]$. Sei g einer der irreduziblen Faktoren. Wir bilden den Körper $\mathbf{L} := \mathbf{K}[t]/(g)$. Wir zeigen nun, dass $t + (g)$ eine Nullstelle von f ist[1]. Dazu berechnen wir $\overline{f}(t+(g)) = \sum_{i=0}^{\deg f} f_i \cdot (t+(g))^i$. Wir wissen, wie man in

[1] $\mathbf{L}$ ist zunächst kein Erweiterungskörper von $\mathbf{K}$, da K keine Teilmenge von L ist. Man kann aber leicht einen Körper $\mathbf{L}'$ angeben, der zu $\mathbf{L}$ isomorph ist, und $\mathbf{K}$ als Unterkörper enthält, indem man in $\mathbf{L}$ jedes konstante Polynom $(k_0, 0, 0, \dots)$ durch k_0 ersetzt.

Quotienten, also in $\mathbf{K}[t]/(g)$ rechnet, und erhalten $\sum_{i=0}^{\deg f} f_i \cdot (t+(g))^i = (\sum_{i=0}^{\deg f} f_i \cdot t^i) + (g)$. Wir wissen, das jedes Polynom $f = (f_0, f_1, f_2, \dots, f_{\deg f}, 0, 0, \dots)$ die Eigenschaft $f = \sum_{i=0}^{\deg f} f_i \cdot t^i$ erfüllt, da ja $t^0 = (1, 0, 0, \dots)$, $t^1 = (0, 1, 0, 0, \dots)$, $t^2 = (0, 0, 1, 0, 0, \dots), \dots$. Also gilt $(\sum_{i=0}^{\deg f} f_i \cdot t^i) + (g) = f + (g)$. Da $g|f$, gilt $f + (g) = 0 + (g)$. Also ist $t + (g)$ eine Nullstelle von f un $\mathbf{L}$. Da f eine Nullstelle l in $\mathbf{L}$ hat, gibt es $h \in \mathbf{L}[t]$, sodass $f = (t - l) \cdot h$. Da h kleineren Grad als f hat, gibt es nach nach Induktionsvorraussetzung einen Erweiterungskörper $\mathbf{M}$ von $\mathbf{L}$, sodass jeder in $\mathbf{M}[t]$ irreduzible Teiler des Polynoms h Grad 1 hat. In $\mathbf{M}[t]$ hat jeder irreduzible Teiler von f also Grad 1. $\square$

Definition 3.2. *Sei* $\mathbf{F}$ *ein Körper, und sei* $f \in F[t]$, $n := \deg f \geq 1$, *und sei* $\mathbf{E}$ *ein Körper.* $\mathbf{E}$ *heißt* Zerfällungskörper *von* f *über* $\mathbf{F}$, *wenn er ein Erweiterungskörper von* $\mathbf{F}$ *ist, und es* $a, e_1, \dots, e_n \in E$ *gibt, sodass*

$$f = a \prod_{i=1}^{n} (t - e_i),$$

und $\mathbf{E}$ *der von* F *und* $\{e_1, e_2, \dots, e_n\}$ *erzeugte Unterkörper von* $\mathbf{E}$ *ist.*

Satz 3.3. *Für jedes nichtkonstante Polynom* f *über einem Körper* $\mathbf{K}$ *gibt es einen Zerfällungskörper von* f *über* $\mathbf{K}$.

4. Irreduzible Polynome über $\mathbb{Q}$

Definition 4.1. *Sei* $a = \sum_{i=1}^{n} a_i t^i \in \mathbb{Z}[t]$, $a \neq 0$. *Wir definieren den* Inhalt von a *durch* $\mathrm{cont}(a) := \mathrm{ggT}(a_0, a_1, \dots, a_n)$.

Lemma 4.2. *Seien* $f, g \in \mathbb{Z}[t] \setminus \{0\}$. *Dann gilt* $\mathrm{cont}(f \cdot g) = \mathrm{cont}(f) \cdot \mathrm{cont}(g)$.

Satz 4.3. *Sei* $f \in \mathbb{Z}[t] \setminus \{0\}$, *seien* $g, h \in \mathbb{Q}[t]$ *so, dass* $f = g \cdot h$, *und seien* $\alpha, \beta \in \mathbb{Z}$ *so, dass* $\alpha\, g \in \mathbb{Z}[t]$ *und* $\beta\, h \in \mathbb{Z}[t]$. *Wir setzen:*

$$\begin{array}{rcl} \gamma & := & \frac{1}{\alpha\,\beta} \cdot \mathrm{cont}(\alpha\, g) \cdot \mathrm{cont}(\beta\, h), \\ g' & := & \frac{1}{\mathrm{cont}(\alpha\, g)}\, \alpha\, g, \\ h' & := & \frac{1}{\mathrm{cont}(\beta\, h)}\, \beta\, h. \end{array}$$

Dann gilt $f = \gamma\,(g' \cdot h')$ *und* $\gamma \in \mathbb{Z}$, $g' \in \mathbb{Z}[t]$, $h' \in \mathbb{Z}[t]$.

Satz 4.4 (Eisenstein Kriterium). *Seien* $n \in \mathbb{N}$, p *Primzahl,* $a = \sum_{i=0}^{n} a_i t^i \in \mathbb{Z}[t]$ *so, dass*

(1) $p|a_0, \dots, p|a_{n-1}$,
(2) $p \not| a_n$,
(3) $p^2 \not| a_0$.

Dann ist a *ein in* $\mathbb{Q}[t]$ *irreduzibles Polynom.*

Satz 4.5. *Sei* $a \in \mathbb{Z}[t]$, $n := \deg a$, *und sei* r *eine rationale Nullstelle von* $a = a_0 t^0 + \cdots + a_n t^n$. *Dann gibt es* $p, q \in \mathbb{Z}$, *sodass* $r = \frac{p}{q}$ *und* $p | a_0$, $q | a_n$.