H24T1A3

geg.: Körper K

$$R = \left\{ \sum_{k=0}^{n} a_k x^k \;\middle|\; n \in \mathbb{N},\ a_0, \dots, a_n \in K,\ a_n = 0_K \right\}$$

bereits gezeigt: R ist ein Teilring des Polynomrings $K[x]$ über dem Körper K

zu (b) Entscheiden Sie, ob das Element $f = x^3$ in R ein irreduzibles Element bzw. ein Primelement ist.

Ang. f ist reduzibel. Dann gibt es eine Zerlegung $f = gh$ in Nicht-Einheiten $g, h \in R$.
Dies ist zugleich eine Zerlegung in $K[x]$.

Dies ist zugleich eine Zerlegung in $K[x]$.

Laut VL ist $K[x]$ ein faktorielles Ring, und x ist (als Pol. vom Grad 1) in $K[x]$ ein irreduzibles Element. Daraus folgt, dass $f = x \cdot x \cdot x$ die im Wesentlichen (bis auf Reihenfolge und Assoziierte) einzige Zerlegung von f in irreduzible Elemente von $K[x]$ ist.
$\Rightarrow$ g und h müssen (bis auf Assoziierte) Potenzen von x sein $g, h \notin R^* \Rightarrow \operatorname{grad}(g), \operatorname{grad}(h) > 0$
Da außerdem $\operatorname{grad}(g) + \operatorname{grad}(h) = \operatorname{grad}(f) = 3$ sein muss, kann nach evtl. Vertauschung von g und h $\operatorname{grad}(g) = 1$, $\operatorname{grad}(h) = 2$ gilt

kein faktorieller Ring.

Insgesamt ist g also assoziiert zu $x \Rightarrow \exists c \in K^\times$ mit $g = cx$ aber: $cx \notin R$ ↯

Also ist f kein reduzibles Element. außerdem $f \neq 0$, und ist auch keine Einheit in $R^\times$, da ansonsten ein $f_1 \in R$ mit $f \cdot f_1 = 1$ existieren würde $\Rightarrow$

$0 = \text{grad}(1) = \text{grad}(f) + \text{grad}(f_1) = 3 + \text{grad}(f_1)$ ↯

Also ist f irreduzibel in R.

Das Element $f = x^3$ ist aber nicht prim, denn:
Sei $a = x^2$, $b = x^4$. Dies sind Elemente von R, und f ist Teiler von $ab = x^6$ wegen $x^6 = f \cdot x^3$ und $x^3 \in R$.
Es gilt aber weder $f \mid a$ noch $f \mid b$, denn:

Ang. $f \mid a \Rightarrow \exists c \in R$ mit $a = c \cdot f \Rightarrow$

$2 = \text{grad}(a) = \text{grad}(c) + \text{grad}(f) = \text{grad}(c) + 3 \Rightarrow$

$3 \leq 2$ ↯ Ang $f \mid b \Rightarrow \exists c \in R$ mit $b = c \cdot f$

$\Rightarrow x^4 = c \cdot x^3 \Rightarrow x \, x^3 = c \cdot x^3$ Kürzungsregel $\Rightarrow x = c$

↯ da x kein Element von R ist

(Polynomringe über Körpern sind Int.-Bereiche)

zu (c) Frage: Ist R ein faktorieller Ring?

Aus der Vorlesung ist bekannt, dass in einem faktoriellen Ring die irreduziblen Elemente genau die Primelemente sind. Da x^3 in R irreduzibel, aber nicht prim ist, ist R also kein faktorieller Ring.

zu (d) ges.: $a \in R$, so dass $I = (a, x^3)$ kein Hauptideal in R ist (mit Nachweis)

Die Elemente von I sind geg durch $I = \{ g \cdot a + h \cdot x^3 \mid g, h \in R \}$, in Abhängigkeit von dem gesuchten Element a.
Ein Hauptideal ist ein Ideal der Form $(u) = \{ gu \mid g \in R \}$, für ein $u \in R$

Beh: $I = (x^2, x^3)$ ist kein Hauptideal in R, d h $a = x^2$ hat die gewünschte Eigenschaft

Ang: I ist Hauptideal in R. Dann gibt es ein $u \in R$ mit $(u) = I = (x^2, x^3)$

$x^2, x^3 \in (u) \Rightarrow \exists\, g, h \in R$ mit $x^2 = gu$
und $x^3 = hu \Rightarrow u$ ist Teiler von x^2 und x^3
in $K[x]$ $\quad u \mid x^2$ in $K[x] \Rightarrow \exists\, c \in K^\times$
mit $u = c$ oder $u = cx$ oder $u = cx^2$
$u = cx$ ist unmöglich, da $cx \notin R$
Ang. $u = cx^2 \Rightarrow x^3 = h \cdot cx^2 \Rightarrow hc = x$
$\Rightarrow h = c^{-1}x$ ↯ da $c^{-1}x \notin R$
Ang. $u = c \in K^\times$ Auch dies ist unmöglich, da
die Elemente in $I = (x^2, x^3)$ alle die Form $g \cdot x^2 +$
$h \cdot x^3$ haben und somit der konstante Term immer
gleich 0 ist. $\rightarrow c \notin I$ ↯
also: I ist kein Hauptideal in R. □

Übung: Zeigen Sie, dass die folgenden Ideale I in den jeweiligen Ringen R keine Hauptideale sind

(a) $R = \mathbb{Z}[x]$, $I = (2, x)$

(b) $R = \mathbb{Q}[x, y]$, $I = (x, y)$

Def: Ein Teilring K eines Rings R heißt Teilkörper, wenn für alle $a \in K$ mit $a \neq 0$ das Element a ein Einheit in R ist und $a^{-1} \in K$ gilt

Bsp: Für jeden Körper K ist K ein Teilkörper des Polynomrings $K[x]$

Erinnerung: Sei $L|K$ eine Körpererweiterung (d.h. K ein Teilkörper von L). Dann ist durch $K \times L \to L$, $(a, x) \mapsto ax$ auf K die Struktur eines **K-Vektorraums** definiert. Dessen Dimension wird als Grad $[L:K]$ der Erweiterung bezeichnet.

Beispiel: $\mathbb{C}$ ist ein 2-dim. $\mathbb{R}$-Vektorraum ($\{1, i\}$ ist eine Basis)
Es gilt also $[\mathbb{C}:\mathbb{R}] = 2$.

H25T3A3

Sei R ein Integritätsbereich, K ein Teilkörper von R, und R sei ein endlich-dim. K-Vektorraum.

(a) Zeigen Sie, dass R unter diesen Voraussetzungen ein Körper ist

Sei $r \in R$ mit $r \neq 0_R$. z.zg: r ist invertierbar, also eine Einheit in R

Da R als K-Vektorraum endl.-dim. ist, ist die Menge $\{1, r, \dots, r^{n-1}\}$ für hinreichend großes $n \in \mathbb{N}$ linear abhängig. Sei $n \in \mathbb{N}$ minimal mit dieser Eigenschaft. Auf Grund der linearen Abhängigkeit gibt es Elemente $c_0, \dots, c_{n-1} \in K$, nicht alle gleich null, mit $c_0 + c_1 r + \dots + c_{n-1} r^{n-1} = 0_K$

$\Rightarrow c_1 r + \dots + c_{n-1} r^{n-1} = -c_0$

1. Fall: $c_0 \neq 0$

$$\Rightarrow 1 = \left(-\frac{c_1}{c_0}\right) r + \dots + \left(-\frac{c_{n-1}}{c_0}\right) r^{n-1}$$

$$= r\left(\left(-\frac{c_1}{c_0}\right) + \dots + \left(-\frac{c_{n-1}}{c_0}\right) r^{n-2}\right)$$

Die Gleichung zeigt, dass r invertierbar ist

2. Fall: $c_0 = 0$

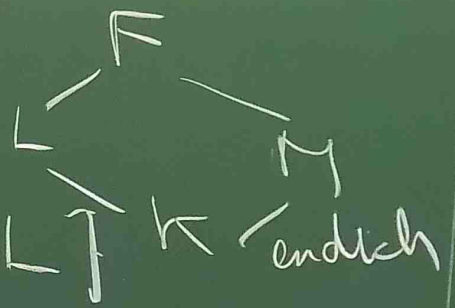
Dann gilt $c_1 r + \dots + c_{n-1} r^{n-1} = 0_K$

$$\Rightarrow r(c_1 + \dots + c_{n-1} r^{n-2}) = 0_K$$

$$r \neq 0_K \Rightarrow c_1 + \dots + c_{n-1} r^{n-2} = 0_K$$ ↯ zur Minimalität

Rückwärts von n.

(b) Sei $F|K$ eine Körpererweiterung und L und M Zwischenkörper von $F|K$.



Sei $R = \{ \sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N}_0, a_i \in M, b_i \in L \}$

Ohne Beweis darf verwendet werden, dass R ein Teilring des Körpers LM ist (wobei LM den kleinsten Zwischenkörper von $F|K$ bezeichnet, der $L \cup M$ enthält)

Zeigen Sie, dass R ein endl.-dim. L-Vektorraum ist, falls die Erweiterung $M|K$ endlich ist.

Zeige zunächst: R ist ein L-Vektorraum

Da R ein Teilring von LM ist, ist $(R, +)$

eine abelsche Gruppe. Betrachte die Abb.
$L \times R \to F$ gegeben durch $(l, r) \mapsto lr$.
Für jedes $l \in L$ und $r \in R$ gilt $lr \in R$, denn:
$r \in R \Rightarrow \exists\, n \in \mathbb{N}_0, a_1, \dots, a_n \in M, b_1, \dots, b_n \in L$
mit $r = \sum_{i=1}^{n} a_i b_i \Rightarrow lr = \sum_{i=1}^{n} a_i (l b_i)$ mit
$l b_i \in L$ (da L Teilkörper von F) $\Rightarrow lr \in R$
Also erhalten wir durch $(l, r) \mapsto lr$ eine Abbildung
$L \times R \to R$. Noch zu überprüfen:
Für alle $l, l' \in L$, $r, r' \in R$ gilt $(l + l')r = lr + l'r$, $l(r + r') = lr + lr'$, $(ll')r = l(l'r)$
und $1_L \cdot r = r$.

Die ersten beiden Gleichungen gelten auf Grund der Distributivgesetze in F, die dritte auf Grund des Assoziativgesetzes der Multiplikation in F und die Gleichung $1_L \cdot r = r$, weil das Einselement in L zugleich das Einselement in F ist. Insgesamt liefert die Abbildung auf R also die Struktur eines L-Vektorraums.

noch z.Zg.: Dieser Vektorraum ist endlich-dim.

Da $M \mid K$ endlich ist, gibt es eine endliche Basis $B = \{m_1, \dots, m_s\}$ von M als K-Vektorraum.

Beh.: B ist Erzeugendensystem von R als L-Vektorraum (daraus folgt, dass die Dimension höchstens $|B|$ ist, insb. endlich).

zu überprüfen: $\langle B \rangle_L = R$

„$\subseteq$" $v \in \langle B \rangle_L \Rightarrow \exists\, a_1, \dots, a_s \in L$ mit

$v = \sum_{i=1}^{s} a_i m_i \quad a_i \in L,\ m_i \in M \Rightarrow v \in R$

„$\supseteq$" Sei $r \in R \Rightarrow \exists\, n \in \mathbb{N}_0,\ a_1, \dots, a_n \in L,$

$b_1, \dots, b_n \in M$ mit $r = \sum_{i=1}^{n} a_i b_i$

Da $\langle B \rangle_L$ ein Untervektorraum von F ist, genügt es, $a_i b_i \in \langle B \rangle_L$ für $1 \leq i \leq n$ zu überprüfen

$b_i \in M$, B Basis von M als K-Vektorraum

$\Rightarrow \exists\, c_1, \dots, c_s \in K$ mit $b_i = \sum_{j=1}^{s} c_j m_j$

$\Rightarrow a_i b_i = \sum_{j=1}^{s} (c_j a_i) b_i \in \langle B \rangle_L$

($c_j a_i \in L$, $b_i \in B$)

Aufgabe H25T3A3 (c)

zu zeigen:
Unter den Voraussetzungen von Teil (b) gilt $[ML : L] \leq [M : K]$.

Als Teilring des Körpers F ist R ein Integritätsbereich. In Teil (b) wurde gezeigt, dass R ein endlich-dimensiomaler L-Vektorraum ist. Sowohl L als auch M ist eine Teilmenge von R. Denn jedes Element $a \in L$ kann in der Form $a = \sum_{k=1}^{1} a_1 b_1$ dargestellt werden, mit $a_1 = a$ und $b_1 = 1_M$, und der Nachweis von $M \subseteq R$ läuft analog.

Da L ein Körper ist, folgt aus $L \subseteq R$, dass es sich um einen Teilkörper von R handelt. Nach Teil (a) ist R somit ebenfalls ein Körper, darüber hinaus ein Teilkörper von F, der $L \cup M$ als Teilmenge enthält. Daraus folgt $ML \subseteq R$.

Laut Angabe gilt außerdem $R \subseteq ML$, insgesamt also $R = ML$. Die Basis B von M als K-Vektorraum aus Teil (b) definiert ist ein Erzeugendensystem von R als L-Vektorraum, wie dort gezeigt wurde. Wegen $R = ML$ folgt daraus $[ML : L] \leq |B| = [M : K]$.