Übung zu Algebraische und Geometrische Strukturen in der Mathematik, SoSe 2014

2. Übungsblatt – Lösungsskizze

Aufgabe P5

Wir zeigen zunächst, dass

$$X := \left\{ \frac{p(a)}{q(a)} \mid p, q \in k[X] \text{ und } q(a) \neq 0 \right\}$$

ein Teilkörper von E ist. Offenbar gilt $0, 1 \in X$. Außerdem impliziert $q(a) \neq 0$ und $q'(a) \neq 0$ dass $(q \cdot q')(a) \neq 0$. Damit sind

$$\frac{p(a)}{q(a)} + \frac{p'(a)}{q'(a)} = \frac{(p \cdot q' + p' \cdot q)(a)}{(q \cdot q')(a)} \quad \text{und} \quad -\frac{p(a)}{q(a)} = \frac{(-p)(a)}{q(a)},$$

ebenso wie

$$\frac{p(a)}{q(a)} \cdot \frac{p'(a)}{q'(a)} = \frac{(p \cdot p')(a)}{(q \cdot q')(a)} \quad \text{und} \quad \left(\frac{p(a)}{q(a)}\right)^{-1} = \frac{q(a)}{p(a)} \text{ falls } p(a) \neq 0$$

in X enthalten. Damit ist X ein Teilkörper. Da dieser a enthält gilt also

$$k(a) = \bigcap \{F \subseteq E \mid F \text{ ist Teilkörper und } a \in F\} \subseteq X.$$

Ist andererseits $F \subseteq E$ ein Teilkörper, der a enthält, dann folgt $p(a) \in F$ für alle $p \in k[X]$, da $p(a)$ nur aus Summen und Produkten von Elementen aus F entsteht. Da F auch abgeschlossen unter dem Bilden von multiplikativen Inversen ist folgt auch $\frac{1}{q(a)} \in F$ für $q \in k[X]$ mit $q(a) \neq 0$. Also enthält F die Menge X. Demnach gilt

$$X \subseteq k(a) = \bigcap \{F \subseteq E \mid F \text{ ist Teilkörper und } a \in F\}.$$

Aufgabe P6

1. Sei F ein Zwischenkörper mit $k \subseteq F \subseteq E$. Nach der Gradformel gilt

   $$[E : k] = [E : F] \cdot [F : k] = p$$

   für p prim. Damit folgt sofort $[E : F] = 1$ oder $[F : k] = 1$ und daher $F = k$ oder $F = E$, es gibt also keinen echten Zwischenkörper.

2. Es gilt offenbar $k \subseteq k(\alpha) \subseteq E$ (warum?). Der erste Aufgabenteil liefert $k = k(\alpha)$ oder $E = k(\alpha)$. Da $\alpha \notin k$ ist, ist $k \neq k(\alpha)$ und es folgt die Behauptung.

Aufgabe P7

1. Wir zeigen gleich die Verallgemeinerung auf unendliche Schnitte, daraus folgt dann der Fall für je zwei Äquivalenzrelationen (ÄRen). Wir müssen zeigen, dass $\bigcap_{i\in I} R_i$ *reflexiv, symmetrisch* und *transitiv* ist. Weil die R_i für jedes $i \in I$ nach Voraussetzung ÄRen sind, gilt $(x, x) \in R_i$ für alle $x \in X$ und alle $i \in I$. Also auch $(x, x) \in \bigcap_{i\in I} R_i$ und die Relation ist *reflexiv*.
   Sei für die *Symmetrie* $(x, y) \in \bigcap_{i\in I} R_i$ mit $x, y \in X$ vorgegeben. Dann aber auch $(x, y) \in R_j$ für alle $j \in I$, da natürlich $\bigcap_{i\in I} R_i \subseteq R_j$ gilt. Weil die R_j ÄRen sind, muss für alle $j \in I$ folgen: $(y, x) \in R_j$ und damit auch $(y, x) \in \bigcap_{i\in I} R_i$. Die *Transitivität* zeigt man genauso.

2. Wir definieren: Die *von einer Teilmenge* $P \subseteq X \times X$ *erzeugte* ÄR als die kleinste ÄR bezüglich "$\subseteq$", die P enthält, d.h. die Äquivalenzrelation Q definiert als

$$Q := \bigcap \{T \subseteq X \times X \mid P \subseteq T \,\text{und}\, T \text{ ist ÄR}\}.$$

3. Die von der leeren Menge erzeugte ÄR ist nach Aufgabenteil (2) gerade

$$N := \{(x, x) | x \in X\}.$$

   Es ist klar, dass dies eine ÄR ist und zwar die *kleinste* ÄR auf X (warum?). Die Ordungsrelation "$\leq$" erzeugt für natürliche Zahlen n, m dagegen die volle ÄR $M := \mathbb{N}\times\mathbb{N}$, denn für $m, n \in \mathbb{N}$ gilt stets $m \leq n$ oder $n \leq m$. Aufgrund der Symmetrie muss M dann auch alle Tupel natürlicher Zahlen enthalten.

   Die Frage nach der ÄR auf der Menge aller Menschen ist natürlich in einem mathematischen Sinne nicht wohldefiniert, deshalb müssen wir eine Annahme machen: Jeder Erwachsene Mensch kennt das Regierungsoberhapt seines Staates (dass das wiederum eine unrealistische Annahme ist sei einmal dahingestellt). Da alle Regeirungschefs sicher den Regierungschef der USA kennen gilt für jeden Menschen a

$$a \sim_{\text{kennt}} \text{Regierungsoberhaupt des Staates von } a \sim_{\text{kennt}} \text{Regierungsoberhaupt der USA}$$

   da die erzeugte ÄR transitiv und symmetrisch sein ist somit die hier erzeugte Äquivalenzrelation ebenfalls die volle.

Aufgabe H4

Wir erinnern uns daran, dass der Grad eines Polynoms $p = \sum_{i=0}^{n} a_i X^i \in k[X] \setminus \{0\}$ das größte $i \leq n$ ist, sodass $a_i \neq 0$. Dann folgen die behaupteten Gradformeln daraus, dass

$$\left(\sum_{i=0}^{n} a_i X^i\right) + \left(\sum_{i=0}^{n} b_i X^i\right) = \sum_{i=0}^{n} (a_i + b_i) X^i$$

und

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot \left(\sum_{i=0}^{n} b_i X^i\right) = \sum_{i=0}^{2n} \left(\sum_{k+j=i} a_k b_j\right) X^i$$

wobei $a_i, b_i \in k$ für alle $i \leq n$. Für die multiplikative Formel benutzen wir dabei, dass k als Körper nullteilerfrei ist, d.h., wenn $a, b \in k$, sodass $a \neq 0$ und $b \neq 0$, dann ist $a \cdot b \neq 0$.

Sei $(k[X])^\times$ die Menge der invertierbaren Elemente von $k[X]$. Dann behaupten wir, dass

$$(k[X])^\times = \{p \in k[X] \setminus \{0\} \mid \deg(p) = 0\}$$

gerade die konstanten und von Null verschiedenen Polynome sind. Es ist klar, dass $(k[X])^\times \supseteq \{p \in k[X] \setminus \{0\} \mid \deg(p) = 0\}$ (Warum?). In die andere Richtung nehmen wir ein Polynom $p \in (k[X])^\times$. Dann ist p nicht das Nullpolynom und es gibt ein Polynom $q \in k[X]$, sodass $p \cdot q = 1$. Aber dann gilt auch

$$\deg(p) + \deg(q) = \deg(p \cdot q) = \deg(1) = 0.$$

Daraus folgt, dass $\deg(p) = 0$.
Insbesondere kann $k[X]$ kein Körper sein, da $(k[X])^\times \neq (k[X] \setminus \{0\})$.

Aufgabe H5

1. Aus $v \in E$ und $k \subseteq E$ folgt direkt, dass

   $$k(v) = \bigcap \{F \subseteq \mathbb{C} \mid k \subseteq F,\, v \in F \text{ and } F \text{ ist Körper}\} \subseteq E.$$

2. „⇒“: Wenn $k(v) = k(w)$, so gilt insbesondere, dass $v \in k(w)$ und somit gibt es $d_0, d_1 \in k$, sodass $v = d_0 + d_1 \cdot w$. Durch Quadrieren erhalten wir daraus, dass

   $$v^2 = (d_0 + d_1 \cdot w)^2 = d_0^2 + 2d_0d_1w + w^2.$$

   Somit gilt, dass $2d_0d_1w = w^2 - d_0^2 - v^2$. Da $v^2, d_0^2, w^2 \in k$ folgt daraus, dass $2d_0d_1w \in k$. Da $2, d_0, d_1 \in k$ aber $w \notin k$ muss gelten, dass $d_0d_1 = 0$ und somit $d_0 = 0$ oder $d_1 = 0$. Aber $d_1 = 0$ kann nicht gelten, da ansonsten $v = d_0$ in k enthalten wäre, im Widerspruch zur Annahme. Daraus folgt $d_0 = 0$, $d_1 \neq 0$ und $v = d_1 \cdot w$.

   „⇐“: Wenn es ein $c \in k \setminus \{0\}$ gibt, sodass $v = c \cdot w$. Somit folgt $v \in k(w)$ und $w \in k(v)$ und somit schließlich $k(w) = k(v)$.

3. Es ist klar, dass $(\sqrt{2} + \sqrt{3}) \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Somit ist $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Für die andere Richtung rechnen wir in $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, dass

   $$\sqrt{6} = \frac{1}{2} \cdot [(\sqrt{2} + \sqrt{3})^2 - 5]$$

   und somit $\sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Wir erhalten nun, dass $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, indem wir rechnen, dass

   $$\sqrt{3} = (3 - \sqrt{6}) \cdot (\sqrt{2} + \sqrt{3})$$

   Hieraus erhalten wir auch direkt, dass $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, da $\sqrt{2} = (\sqrt{2} + \sqrt{3}) - \sqrt{3}$. Somit folgt, dass $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

4. Es ist $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Somit genügt es zu zeigen, dass $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. Zunächst wissen wir, dass $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Wir bemerken, dass $3 \in \mathbb{Q}(\sqrt{2})$, aber $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, denn wäre $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, so wäre $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2})$ und somit nach Aufgabe P6 sogar $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2})$. Dies ist aber im Widerspruch zu Aufgabe H5.2, da $\sqrt{\frac{3}{2}} \notin \mathbb{Q}$. Somit ist $\mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ und $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist eine Erweiterung von $\mathbb{Q}(\sqrt{2})$ durch eine Quadratwurzel, sodass $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ gilt. Nach der Gradformel folgt nun, dass $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$.

Aufgabe H6

1. Man überlegt sich zunächst, dass Φ_F der *Einsetzungshomomorphismus* ist, der für die Variable X den Endomorphismus F einsetzt. Insofern ist $\Phi_F(X^2+1) = F^2 + id$, und man rechnet (E_3 sei die Einheitsmatrix):

$$\begin{pmatrix} 1 & 0 & 6 \\ 0 & \pi & 0 \\ 0 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 6 \\ 0 & \pi & 0 \\ 0 & 0 & 2 \end{pmatrix} + E_3 = \begin{pmatrix} 1 & 0 & 12 \\ 0 & \pi^2 & 0 \\ 0 & 0 & 4 \end{pmatrix} + E_3 = \begin{pmatrix} 2 & 0 & 12 \\ 0 & \pi^2+1 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

2. Es gilt für Polynome $P, Q \in k[X]$ und für $c \in k$ (nach Definition):

$$\Phi_F(P+Q) = \Phi_F(\sum_i (a_i + b_i)X^i) = \sum_i a_i F^i + \sum_i b_i F^i = \Phi_F(P) + \Phi_F(Q)$$

$$c\Phi_F(P) = c\sum_i a_i F^i = \sum_i c a_i F^i = \Phi_F(cP)$$

   Somit ist Φ_F eine k-lineare Abbildung. Die Multiplikation von Elementen aus $k[F]$ prüft man genauso nach und erhält damit, dass Φ_F ein Ringhomomorphismus ist [1]. Da das Bild einer linearen Abbildung ein Untervektorraum des Bildraumes ist und das Bild eines Ringhomomorphismus ein Unterring des Bildringes ist folgt hieraus schon, dass $k[F] = \mathrm{im}(\Phi_F)$ ein k-Vektorraum und ein Ring ist.

3. Zunächst rekapitulieren wir aus der LA, dass für V wie in der Behauptung gilt:

$$\dim_k(\mathrm{End}_V) = \dim_k(k^{n\times n}) = n^2 < \infty.$$

   Damit sind wir (fast) fertig, denn $k[X]$ hat unendliche Dimension und End_V endliche, insbesondere kann dann $\ker(\Phi_F)$ nicht trivial sein. Damit existiert mindestens ein nicht-triviales Polynom P, sodass $\Phi_F(P) = 0$. Dieses können wir o.B.d.A. als normiert voraussetzen (teile andernfalls durch den Koeffizienten $a_n \in k$). Der Grad von P kann nicht größer als $\dim_k(\mathrm{End}_V)$ sein, weil die $\Phi_F(X^0), ..., \Phi_F(X^{n^2})$ in End_V linear abhängig sind. (Schneller und einfacher geht es so: Da $\dim_k(\mathrm{End}_V) = n^2$, gibt es $a_i \in k$ für $i \leq n$, sodass $F^{n^2} = \sum_{i=0}^{n^2-1} a_i F^i$ und somit $F^{n^2} - \sum_{i=0}^{n^2-1} a_i F^i = 0$. Damit ist $X^{n^2} - \sum_{i=0}^{n^2-1} a_i X^i$ ein normiertes Polynom mit der geforderten Eigenschaft.)

[1] In *S. Bosch, Lineare Algebra, S. 171* wird der Beweis gleich für einen Homomorphismus von k-Algebren geliefert. Dies hatten wir in der Vorlesung jedoch nicht definiert.