Lösungsbeispiele zu Übungsblatt 13

Aufgabe 3: Sei $K = \mathbb{Z}/p\mathbb{Z}$ mit Primzahl p und $L := K(x, y)$ der Körper der rationalen Funktionen in den Unbestimmten x und y. Zeigen Sie:

(a) $L^p = K(x^p, y^p)$ und $[L : L^p] = p^2$.

(b) $L = \bigcup_{a \in L \setminus L^p} L^p(a)$ und dabei ist $[L^p(a) : L^p] = p$.

(c) Ein Vektorraum **über einem Körper mit unendlich vielen Elementen** ist keine Vereinigung endlich vieler echter Unterräume.

(d) $L|L^p$ besitzt unendlich viele Zwischenkörper.

(a) Da bei dieser Aufgabe ein Körper der Charakteristik p vorliegt, gilt $(a+b)^p = a^p + b^p$ für alle $a, b \in L$. Insbesondere gilt für Polynome aus $K[x, y]$ die Identität

$$\begin{aligned} (f(x,y))^p &= (\sum_{k,l \geq 0} f_{kl} x^k y^l)^p \\ &= \sum_{k,l \geq 0} (f_{kl})^p (x^p)^k (y^p)^k \\ &= \sum_{k,l \geq 0} f_{kl} (x^p)^k (y^p)^k \in K[x^p, y^p] \end{aligned}$$

Beachte, dass der Frobenius-Homomorphismus $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $\alpha \mapsto \alpha^p$ die Identität ist. (Folgt aus $\alpha^{p-1} \equiv 1 \pmod p$ (Fermat) durch Multiplikation mit α.) Damit gilt $(K[x, y])^p = K[x^p, y^p]$.

Da jedes Element von $L = K(x, y)$ als ein Quotient von Polynomen aus $K[x, y]$ darstellbar ist, folgt $L^p = K(x^p, y^p)$.

Um $[L\colon L^p] = p^2$ zu zeigen, verwende zunächst die Gradformel,

$$[L\colon L^p] = [K(x, y)\colon K(x^p, y)] \cdot [K(x^p, y)\colon K(x^p, y^p)] \ .$$

Beide Faktoren haben den Erweiterungsgrad p: Der Körper $K(x, y)$ ist eine einfache, algebraische Erweiterung von $K(x^p, y)$, denn $K(x, y) = K(x^p, y)(x)$ und $z^p - x^p \in K(x^p, y)[z]$ ist ein Polynom mit Nullstelle x. Dass der Erweiterungsgrad genau p ist, folgt aus der Irreduzibilität des angegebenen Polynoms: Im Polynomring $K[x^p, y]$ ist x^p ein irreduzibles Element. Damit lässt sich das Eisenstein-Kriterium auf $z^p - x^p \in (K[x^p, y])[z]$ anwenden. Der Satz von Gauß liefert die Irreduzibilität über $K(x^p, y)$.

Analog zeigt man, dass der zweite Faktor den Erweiterungsgrad p besitzt.

(b) Zunächst ist die Gleichheit $L = \bigcup_{a \in L \setminus L^p} L^p(a)$ zu zeigen. Für alle $a \in L$ gilt $L^p(a) \subseteq L$, also die Inklusion $\supseteq$. Für die umgekehrte Inklusion sind zwei Fälle zu unterscheiden. Ist $a \in L \setminus L^p$, so gilt $a \in L^p(a)$. Ist $b \in L^p$, so gilt $b \in L^p(a)$ für beliebiges $a \in L \setminus L^p$; ein solches existiert, da $[L\colon L^p] \neq 1$.

Nun zum Erweiterungsgrad $[L^p(a)\colon L^p] = p$. Da $L^p(a)$ ein Zwischenkörper von $L|L^p$ ist, ist der Erweiterungsgrad ein Teiler von p^2. Da es sich um eine einfache Erweiterung handelt und $z^p - a^p \in L^p[z]$ die Nullstelle a besitzt, folgt $[L^p(a)\colon L^p] \leq p$. Da $a \in L \setminus L^p$ vorausgesetzt ist, folgt $[L^p(a)\colon L^p] > 1$.

(c) Ohne die (untere) Einschränkung an die Elementeanzahl ist die Aussage falsch. Ein Gegenbeispiel ist gegeben durch den zweidimensionalen Vektorraum $(\mathbb{Z}/2\mathbb{Z})^2$: Er ist Vereinigung der Geraden

$$\{(0,0),(0,1)\} \quad , \quad \{(0,0),(1,0)\} \quad , \quad \{(0,0),(1,1)\} \ .$$

Wir setzen nun einen unendlichen Körper K voraus. Als Widerspruchsannahme sei $V = U_1 \cup \ldots \cup U_n$, wobei oBdA keiner der echten Unterräume U_i in der Vereinigung der anderen Unterräume enthalten sein soll. Dann gibt es ein $x_1 \in U_1 \setminus (U_2 \cup \ldots \cup U_n)$ und ein $x_n \notin U_1$. Betrachte die Gerade $g := \{x_n + \lambda x_1 \mid \lambda \in K\}$. Sie hat unendlich viele Elemente.

Da $x_n \notin U_1$, gilt $g \cap U_1 = \emptyset$. Weiter wollen wir zeigen, dass $g \cap U_i$ auch höchstens einelementig ist für alle $1 < i \leq n$. Seien $x_n + \alpha x_1 = x_n + \beta x_1 \in U_i$. Dann gilt $(\alpha - \beta)x_1 \in U_i$. Nach Voraussetzung ist $x_1 \notin U_i$, also folgt $\alpha = \beta$.

Damit enthält $g = g \cap V = (g \cap U_1) \cup \ldots \cup (g \cap U_n)$ höchstens $n-1$ Elemente im Widerspruch dazu, dass g unendlich viele Elemente enthält.

(d) In (b) wurde gezeigt, dass L eine Vereinigung von echten Zwischenkörpern ist. Nach (c) muss es also unendlich viele davon geben.

Aufgabe 4: Wahr oder falsch?

(a) Jeder injektive K-Homomorphismus ist ein K-Automorphismus.

Falsch: Die Einbettung $K \to K(x)$ für $x \notin K$ ist nicht surjektiv.

(b) Jede endliche Körpererweiterung hat eine normale Hülle.

Wahr: Jede endliche Erweiterung ist algebraisch und jede algebraische Erweiterung besitzt eine normale Hülle.

(c) Jede Erweiterung eines Körpers mit Charakteristik 0 ist normal.

Falsch: $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ ist nicht normal.

(d) Eine Körpererweiterung mit Galoisgruppe der Ordnung 1 ist normal.

Falsch: $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}) = \{id\}$.

(e) Eine endliche, separable, normale Körpererweiterung besitzt eine endliche Galoisgruppe.

Wahr: Unter den Voraussetzungen ist der endliche Erweiterungsgrad gleich der Ordnung der Galoisgruppe.

(f) Jede Galoisgruppe ist abelsch.

Falsch: Gegenbeispiel s. Aufgabe 2.

(g) Eine Galoiserweiterung $L|K$ mit $[L:K] = n$ besitzt eine Galoisgruppe der Ordnung n.

Wahr: Für eine Galoiserweiterung gilt $[L\colon K] = |\mathrm{Gal}(L|K)|$.

(h) Die Galoisgruppe einer normalen Körpererweiterung ist zyklisch.

Falsch: Gegenbeispiel s. Aufgabe 2.