G. Nebe, M. Künzer

Übungen Algebra II, Sommersemester 03

Lösung 8

Aufgabe 1.

(1) Wir zeigen, daß die Summe zweier nilpotenter Ideale $N', N'' \subseteq A$ wieder ein nilpotentes Ideal bildet. Damit hat ein nilpotentes Ideal maximaler K-Dimension die verlangte Maximalitätseigenschaft.

Es ist zu zeigen, daß $(N' + N'')^m = 0$ für ein $m \geq 1$. Ein Element einer derartigen Idealpotenz ist von der Form $x := (n'_1 + n''_1)(n'_2 + n''_2) \cdots (n'_m + n''_m)$ mit $n'_i \in N'$ und $n''_i \in N''$. Sei $N'^{m'} = 0$ und sei $N''^{m''} = 0$. Ist $m \geq m' + m''$, so enthält nach Ausmultiplizieren des Ausdrucks für x jeder Summand mindestens m' Faktoren in N' oder mindestens m'' Faktoren in N''. Ersterenfalls verwendet man $A \cdot N' \cdot A \subseteq N'$, um das Produkt in ein Produkt aus $\geq m'$ Elementen von N' umzuschreiben, welches nach Voraussetzung verschwindet. Zweiterenfalls genauso mit N''.

(2+4) Sei J der Schnitt aller maximalen Linksideale von A. Es ist J ein Linksideal. Wir behaupten, daß J ein Ideal ist. Sei $x \in J$, sei $a \in A$ und sei L ein maximales Linksideal. Zu zeigen ist $xa \in L$. Sei $A \xrightarrow{f} A$, $y \longmapsto ya$, es ist f eine A-linkslineare Abbildung. Wir behaupten, daß $(L)f^{-1}$ entweder gleich A oder maximales Linksideal ist. In der Tat ist $A/(L)f^{-1} \longrightarrow A/L$, $y \longmapsto ya$, injektiv, und A/L einfach, also $A/(L)f^{-1}$ gleich 0 oder einfach. In beiden Fällen ist $x \in (L)f^{-1}$, und somit $xa \in L$.

Wir behaupten $J \subseteq \mathrm{Jac}(A)$, i.e. J nilpotent. Sei

$$A = X_0 \supset X_1 \supset X_2 \cdots \supset X_k = 0$$

eine maximale Kette von Linksidealen, i.e. nicht verfeinerbar, oder aber, mit X_i/X_{i+1} einfach stets. Es genügt, $J(X_i/X_{i+1}) = 0$ zu zeigen, denn dann ist $J^k = J^k X_0 = 0$. Es genügt also, für S einen einfachen Linksmodul $JS = 0$ zu zeigen. Sei $s \in S \setminus \{0\}$, sei $L = \{a \in A \mid as = 0\}$. Es wird $A/L \xrightarrow{\sim} S$, $a \longmapsto as$, mithin L maximales Linksideal, und somit $J \subseteq L$, und also $Js = 0$.

Wir behaupten $\mathrm{Jac}(A) \subseteq J$. Ist L ein maximales Linksideal, so haben wir $\mathrm{Jac}(A) \subseteq L$ zu zeigen. Da A/L einfach ist, bleibt $\mathrm{Jac}(A)(A/L) = A/L$ auszuschließen. Daraus folgte aber $0 = \mathrm{Jac}(A)^m(A/L) = A/L$ für ein $m \geq 1$, was in der Tat nicht möglich ist.

Also $\mathrm{Jac}(A) = J$, wie in (4) behauptet wurde. Zu zeigen sind nun noch zwei Dinge. Zum ersten, daß kein Ideal N, welches echt in $\mathrm{Jac}(A)$ enthalten ist, einen halbeinfachen Quotienten haben kann, und zum zweiten, daß $A/\mathrm{Jac}(A)$ halbeinfach ist.

Ersteres läuft wegen $\mathrm{Jac}(A)/N$ nilpotentes Ideal in A/N darauf hinaus, zu zeigen, daß eine halbeinfache endlichdimensionale Algebra kein nilpotentes Ideal ungleich 0 haben kann. Argument mit Wedderburn: eine halbeinfacher noetherscher Ring enthält nur idempotente Ideale, da ein Matrixring über einem Schiefkörper nur die beiden trivialen Ideale hat. Argument ohne Wedderburn: Sei B halbeinfach, und sei $M \subseteq B$ ein nilpotentes Ideal. Wenn der B/M-linkslineare Epimorphismus $B \longrightarrow B/M$ aufspaltet, wird $1 \in B/M$ auf ein Element $1 - x \in B$ mit $x \in M$ geschickt, welches wegen $B/M \longrightarrow B$ wohldefiniert zugleich von M annulliert wird. Da $(1-x)(1+x+\cdots+x^k) = 1$ für ein $k \geq 1$, würde dann M auch die 1 annullieren, i.e. $M = 0$.

Zu zweiterem bemerken wir, daß $\mathrm{Jac}(A/\mathrm{Jac}(A)) = 0$. Denn gäbe es ein Ideal $I \supseteq \mathrm{Jac}(A)$, welches modulo $\mathrm{Jac}(A)$ nilpotent ist, so wäre $I^n \subseteq \mathrm{Jac}(A)$ für ein $n \geq 0$, also $I^{nm} \subseteq \mathrm{Jac}(A)^m = 0$ für ein $m \geq 0$, was $I \subseteq \mathrm{Jac}(A)$ impliziert. Wir haben also zu zeigen, daß $\mathrm{Jac}(A) = 0$ nach sich zieht, daß A halbeinfach ist. Nun ist aber wegen A endlichdimensional $0 = \mathrm{Jac}(A) = L_1 \cap \cdots \cap L_k$ mit bereits endlich vielen maximalen Linksidealen L_i. Daher gibt es einen Monomorphismus $A \overset{\iota}{\hookrightarrow} \bigoplus_{i \in [1,k]} A/L_i =: X$, $1 \longmapsto (1, \ldots, 1)$ von A-Linksmoduln.

Wir behaupten, daß A ein direkter Summand von X ist. Sei $I \subseteq [1,k]$ maximal mit $A\iota \oplus \bigoplus_{i \in I} A/L_i \subseteq X$ direkt. Wäre $A\iota \oplus \bigoplus_{i \in I} A/L_i \subset X$, so gäbe es ein $j \in [1,k] \smallsetminus I$ mit $A/L_j \not\subseteq A\iota \oplus \bigoplus_{i \in I} A/L_i$, also, wegen A/L_j einfach, $(A/L_j) \cap (A\iota \oplus \bigoplus_{i \in I} A/L_i) = 0$, also $A\iota \oplus \left(\bigoplus_{i \in I} A/L_i\right) \oplus A/L_j$ direkt, Widerspruch. Damit ist $A\iota$ direkter Summand von X.

Insbesondere gibt es einen Epimorphismus $X \longrightarrow A$, und folglich ist A die Summe einfacher Moduln $A = \sum_{i \in [1,l]} S_i$. Wir behaupten, daß jeder einfache Modul projektiv ist. Sei S einfach. Dann gibt es einen Epimorphismus $A \longrightarrow S$ mit Kern Y, und mit dem Argument von eben ist $Y \hookrightarrow A$ ein aufspaltender Monomorphismus, also $A \simeq Y \oplus S$, also S projektiv. (Oder: $\exists\, i \quad S_i \simeq S$ mit Schur.)

Mit dem Satz von Wedderburn ist es egal, ob Links- oder Rechtsmoduln als projektiv nachgewiesen werden, um A halbeinfach nachzuweisen. Sei nun M ein beliebiger A-Linksmodul. Mit Induktion über seine K-Dimension genügt es für M projektiv zu zeigen, daß M einen projektiven direkten Summanden hat. Sei $N \subset M$ ein maximaler Teilmodul von M. Es ist $M \longrightarrow M/N$ ein Epimorphismus auf einen einfachen, und also projektiven Modul. Daher ist in der Tat $M \simeq N \oplus (M/N)$. Es ist somit A halbeinfach gezeigt.

(Man kann sogar zeigen, daß $\mathrm{Jac}(A)$ in jedem Ideal enthalten ist, welches einen halbeinfachen Quotienten hat.)

(3) Nach (1) und (2) ist $\mathrm{Jac}(A)$ charakterisiert als das *einzige* nilpotente Ideal von A mit halbeinfachem Quotienten.

Um dann in der Pierce-Zerlegung für ein Idempotent e die Primitivität zu zeigen, genügt es zu haben, daß eAe keine nichttrivialen Idempotente enthält.

(i) Es ist $A \simeq \mathbf{Q}[X]/(X+1)^2 \times \mathbf{Q}[X]/(X-1)^2 \times \mathbf{Q}[X]/(X^2+1)^2$, und diese direkte Zerlegung entspricht der orthogonalen Zerlegung $1 = e_1 + e_2 + e_3$ mit den Idempotenten

$$
\begin{aligned}
e_1 &= (+3X^7 - 2X^6 + X^5 - 7X^3 + 6X^2 - 5X + 4)/16 \\
e_2 &= (-3X^7 - 2X^6 - X^5 + 7X^3 + 6X^2 + 5X + 4)/16 \\
e_3 &= (X^6 - 3X^2 + 2)/4\,.
\end{aligned}
$$

Es ist $e_iAe_j = 0$ für $i \neq j$, und $e_1Ae_1 \simeq \mathbf{Q}[X]/(X+1)^2$, $e_2Ae_2 \simeq \mathbf{Q}[X]/(X-1)^2$ und $e_3Ae_3 \simeq \mathbf{Q}[X]/(X^2+1)^2$. In allen diesen drei Ringen gibt es genau ein maximales Ideal (viz. $(X+1)$, $(X-1)$ resp. (X^2+1)), also sind in der Tat die drei gefundenen Idempotente primitiv.

Ist A ein kommutativer Ring, so ist $\mathrm{Jac}(A) = \mathrm{Nil}\,(A)$, also $\mathrm{Jac}(A) = (X^4-1)$. Reduktion der Idempotentzerlegung für A modulo (X^4-1) liefert

$$\begin{array}{rcl} \bar{e}_1 & = & (-X^3+X^2-X+1)/4 \\ \bar{e}_2 & = & (+X^3+X^2+X+1)/4 \\ \bar{e}_3 & = & (-X^2+1)/2\ . \end{array}$$

Es ist $\bar{e}_i(A/\mathrm{Jac}(A))\bar{e}_j = 0$ für $i \neq j$, und $\bar{e}_1(A/\mathrm{Jac}(A))\bar{e}_1 \simeq \mathbf{Q}[X]/(X+1) \simeq \mathbf{Q}$, $\bar{e}_2(A/\mathrm{Jac}(A))\bar{e}_2 \simeq \mathbf{Q}[X]/(X-1) \simeq \mathbf{Q}$, $\bar{e}_3(A/\mathrm{Jac}(A))\bar{e}_3 \simeq \mathbf{Q}[X]/(X^2+1) \simeq \mathbf{Q}(i)$. Alle diese drei Ringe sind Körper, also sind in der Tat die drei gefundenen Idempotente primitiv.

(ii) Es ist A einfach, also ohne nichttriviales Ideal. Speziell ist $\mathrm{Jac}(A) = 0$. Es gibt aber sehr wohl nilpotente *Elemente* in A, etwa $\left(\begin{smallmatrix} 0&1&0\\0&0&1\\0&0&0 \end{smallmatrix}\right)$. Die Pierce-Zerlegung von A resultiert aus $e_1 := \mathrm{diag}(1,0,0)$, $e_2 := \mathrm{diag}(0,1,0)$, $e_3 := \mathrm{diag}(0,0,1)$, und es wird $e_iAe_j \simeq \mathbf{Q}$ stets.

(iii) Die Pierce-Zerlegung von A resultiert aus $e_1 := \mathrm{diag}(1,0,0)$, $e_2 := \mathrm{diag}(0,1,0)$, $e_3 := \mathrm{diag}(0,0,1)$, es ist $e_iAe_j = 0$ für $(i,j) \in \{(3,1),(3,2)\}$, und $e_iAe_j \simeq \mathbf{Q}$ sonst.

Es ist $\mathrm{Jac}(A) = \left(\begin{smallmatrix} 0&0&\mathbf{Q}\\0&0&\mathbf{Q}\\0&0&0 \end{smallmatrix}\right) \subseteq \left(\begin{smallmatrix} \mathbf{Q}&\mathbf{Q}&\mathbf{Q}\\\mathbf{Q}&\mathbf{Q}&\mathbf{Q}\\0&0&\mathbf{Q} \end{smallmatrix}\right) = A$, da dies ein nilpotentes Ideal ist, und da $A/\mathrm{Jac}(A) \simeq \mathbf{Q}^{2\times 2} \times \mathbf{Q}$ halbeinfach ist.

In $A/\mathrm{Jac}(A)$ können wir das Bild der obigen Idempotentzerlegung verwenden, und erhalten $\bar{e}_i(A/\mathrm{Jac}(A))\bar{e}_j = 0$ für $(i,j) \in \{(3,1),(3,2),(1,3),(2,3)\}$, und $e_iAe_j \simeq \mathbf{Q}$ sonst.

(iv) Die Pierce-Zerlegung von A resultiert aus $e_1 := \mathrm{diag}(1,1,0)$, $e_2 := \mathrm{diag}(0,0,1)$. Es ist $e_1Ae_1 \simeq \{(a_{i,j})_{i,j} \in \mathbf{Q}^{2\times 2}\ :\ a_{2,1} = 0,\ a_{1,1} = a_{2,2}\}$, $e_2Ae_1 = 0$, $e_1Ae_2 \simeq \left(\begin{smallmatrix} \mathbf{Q}\\\mathbf{Q} \end{smallmatrix}\right)$, und $e_2Ae_2 \simeq \mathbf{Q}$. Für die Primitivität von e_1 merken wir an, daß in einer Zerlegung $\left(\begin{smallmatrix} 1&0\\0&1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a&b\\0&a \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1-a&-b\\0&1-a \end{smallmatrix}\right)$ die Idempotenz von $\left(\begin{smallmatrix} a&b\\0&a \end{smallmatrix}\right)$ bereits $a \in \{0,1\}$ und $2ab = b$ zur Folge hat, woraus wir wiederum $b = 0$ ersehen.

Ferner ist $\mathrm{Jac}(A) = \left(\begin{smallmatrix} 0&\mathbf{Q}&\mathbf{Q}\\0&0&\mathbf{Q}\\0&0&0 \end{smallmatrix}\right)$, da dieses Ideal nilpotent ist, und da $A/\mathrm{Jac}(A) \simeq \mathbf{Q} \times \mathbf{Q}$ halbeinfach ist.

Die Bilder der Idempotente modulo $\mathrm{Jac}(A)$ liefern eine Idempotentzerlegung von $A/\mathrm{Jac}(A)$, mit $\bar{e}_1(A/\mathrm{Jac}(A))\bar{e}_2 = \bar{e}_2(A/\mathrm{Jac}(A))\bar{e}_1 = 0$ und $\bar{e}_1(A/\mathrm{Jac}(A))\bar{e}_1 \simeq \mathbf{Q}$ sowie $\bar{e}_2(A/\mathrm{Jac}(A))\bar{e}_2 \simeq \mathbf{Q}$.

(v) Wir erhalten die Idempotente $e_1 := \mathrm{diag}(1,1,0)$, $e_2 := \mathrm{diag}(0,0,1)$. Es ist $e_1Ae_1 \simeq \{(a_{i,j})_{i,j} \in \mathbf{Q}^{2\times 2}\ :\ a_{2,1} = -a_{1,2},\ a_{1,1} = a_{2,2}\} \simeq \mathbf{Q}(i)$ (mit $\left(\begin{smallmatrix} 0&1\\-1&0 \end{smallmatrix}\right) \longmapsfrom i$), $e_2Ae_1 = 0$, $e_1Ae_2 \simeq \left(\begin{smallmatrix} \mathbf{Q}\\\mathbf{Q} \end{smallmatrix}\right)$, und $e_2Ae_2 \simeq \mathbf{Q}$.

Es ist $\mathrm{Jac}(A) = \left(\begin{smallmatrix} 0&0&\mathbf{Q}\\0&0&\mathbf{Q}\\0&0&0 \end{smallmatrix}\right)$, da dieses Ideal nilpotent ist, und da $A/\mathrm{Jac}(A) \simeq \mathbf{Q}(i) \times \mathbf{Q}$ halbeinfach ist.

Die Bilder der Idempotente modulo $\mathrm{Jac}(A)$ liefern eine Idempotentzerlegung von $A/\mathrm{Jac}(A)$, mit $\bar{e}_1(A/\mathrm{Jac}(A))\bar{e}_2 = \bar{e}_2(A/\mathrm{Jac}(A))\bar{e}_1 = 0$ und $\bar{e}_1(A/\mathrm{Jac}(A))\bar{e}_1 \simeq \mathbf{Q}(i)$ sowie $\bar{e}_2(A/\mathrm{Jac}(A))\bar{e}_2 \simeq \mathbf{Q}$.

(vi) Das Tensorprodukt mit $\mathbf{Q}(i)$ über $\mathbf{Q}$ der Algebra aus (v) gibt

$$A \;\simeq\; \{(a_{i,j})_{i,j} \in \mathbf{Q}(i)^{3\times 3} \mid a_{3,1} = a_{3,2} = 0,\ a_{1,1} = a_{2,2},\ a_{2,1} = -a_{1,2}\}\ ,$$

und diesen Isomorphismus verwenden wir als Identifikation. Wir erhalten die Idempotente $e_1 = \frac{1}{2}\left(\begin{smallmatrix} 1 & i \\ -i & 1 \end{smallmatrix}\right)$ und $e_2 = \frac{1}{2}\left(\begin{smallmatrix} 1 & -i \\ i & 1 \end{smallmatrix}\right)$. Die Pierce-Zerlegung liefert einen Isomorphismus $A \simeq \left(\begin{smallmatrix} \mathbf{Q}(i) & 0 & \mathbf{Q}(i) \\ 0 & \mathbf{Q}(i) & \mathbf{Q}(i) \\ 0 & 0 & \mathbf{Q}(i) \end{smallmatrix}\right)$. Darin ist das Jacobson-Radikal gegeben durch $A \simeq \left(\begin{smallmatrix} 0 & 0 & \mathbf{Q}(i) \\ 0 & 0 & \mathbf{Q}(i) \\ 0 & 0 & 0 \end{smallmatrix}\right)$. Die Bilder der Idempotenten von A in $A/\mathrm{Jac}(A)$ liefern eine Pierce-Zerlegung von $A/\mathrm{Jac}(A) \simeq \mathbf{Q}(i) \times \mathbf{Q}(i) \times \mathbf{Q}(i)$.

Aufgabe 2.

(1) Ist K perfekt, so schränkt der Frobenius $\bar{K} \xrightarrow[\sim]{\mathrm{F}} \bar{K}$, $x \longmapsto x^p$, zu einer Bijektion $K \xrightarrow{\sim} K$ ein. Ist $(x_1, \ldots, x_m)$ linear unabhängig über K und ist $\sum_{i\in[1,m]} \alpha_i x_i^p = 0$ mit $\alpha_i \in K$, so ist auch $\sum_{i\in[1,m]} \alpha_i^{p^{-1}} x_i = 0$, und somit $\alpha_i = 0$ für alle $i \in [1,m]$.

Ist umgekehrt jede Erweiterung $L|K$ separabel, so auch insbesondere $K^{p^{-1}}|K$. Wäre $K \subset K^{p^{-1}}$, so gäbe es ein Tupel $(x_1, \ldots, x_m)$ von Länge $m > 1$ in $K^{p^{-1}}$, welches über K linear unabhängig ist. Es kann nun $(x_1^p, \ldots, x_m^p)$ über K nicht linear unabhängig über K sein, da alle $x_i \in K$ liegen.

(2) (i) $\Longleftrightarrow$ (ii). Die $K^{p^{-1}}$-lineare Abbildung $L \otimes_K K^{p^{-1}} \longrightarrow L^{p^{-1}}$ ist injektiv genau dann, wenn jedes K-linear unabhängige Tupel $(x_1, \ldots, x_m)$ von L, gesehen im Tensorprodukt als $(x_1 \otimes 1, \ldots, x_m \otimes 1)$, auf ein $K^{p^{-1}}$-linear unabhängige Tupel geht, i.e. wenn $(x_1, \ldots, x_m)$ linear unabhängig über $K^{p^{-1}}$ bleibt, i.e. wenn $(x_1^p, \ldots, x_m^p)$ linear unabhängig über K ist.

(ii) $\Longrightarrow$ (iii). Aus (ii) folgt, daß $L \otimes_K K^{p^{-1}}$ ein Integritätsbereich ist, und eine endlichdimensionale nullteilerfreie Ringerweiterung eines Körpers ist selbst ein Köper.

(iii) $\Longrightarrow$ (ii). Ist $L \otimes_K K^{-p}$ ein Körper, so ist jeder Ringmorphismus in einen Ring ungleich dem Nullring injektiv.

(iii) $\Longleftrightarrow$ (iv). Ist $L \otimes_K K^{p^{-1}}$ halbeinfach, so ist es ein Produkt von Körpern. Wir haben zu zeigen, daß ein Idempotent $e = \sum_i x_i \otimes \alpha_i^{-p} \in L \otimes_K K^{p^{-1}}$ trivial ist, i.e. $e = 0$ oder $e = 1$. In der Tat ist $e = e^p = \sum_i x_i^p \otimes \alpha_i = (\sum_i x_i^p \alpha_i) \otimes 1 \in L \otimes 1 \simeq L$, und somit trivial.

(v) $\Longrightarrow$ (iv).

(vi) $\Longleftrightarrow$ (vii). Spaltet $L \otimes_K L \longrightarrow L$ auf, so ist L als direkter Summand von $L \otimes_K L$ projektiv.

(v) $\Longleftrightarrow$ (vii). Sei $L \otimes_K L \longrightarrow L$ aufspaltend als L-L-Bimodulepimorphismus, und sei $\sum_{i\in I} a_i \otimes b_i$ das Bild von 1_L unter der Aufspaltung. Insbesondere ist $\sum_{i\in I} a_i b_i = 1$ und $\sum_{i\in I} c a_i \otimes b_i = \sum_{i\in I} a_i \otimes b_i c$ für alle $c \in L$, letzteres, da $c \cdot 1_L = 1_L \cdot c$ sich im

Bild der Aufspaltung widerspiegelt. Wir haben zu zeigen, daß jeder Epimorphismus $X \xrightarrow{f} Y$ von $L \otimes_K F$-Moduln aufspaltet. Sei $X \xleftarrow{g} Y$ eine F-lineare Aufspaltung, i.e. sei $gf = 1_Y$. Sei

$$\begin{array}{ccc} X & \xleftarrow{\tilde{g}} & Y \\ \sum_{i\in I} a_i((yb_i)g) & \longleftarrow\!\shortmid & y\,. \end{array}$$

Es ist wegen g F-linear $\tilde{g}$ weiterhin F-linear, und es wegen $\sum_{i\in I} a_i b_i = 1$ weiterhin $\tilde{g}f = 1_Y$. Nun ist aber $\tilde{g}$ dazuhin L-linear wegen

$$\begin{array}{rcl} (yc)\tilde{g} & = & \sum_{i\in I} a_i((yb_ic)g) \\ & = & \sum_{i\in I} ca_i((yb_i)g) \end{array}$$

für $c \in L$, da wir eine Operation von $L \otimes_K L$ auf $\mathrm{Hom}_F(Y, X)$ haben derart, daß für $Y \xrightarrow{h} X$, für $a, b \in L$ und $y \in Y$ wird $y((a \otimes b) \cdot h) := a((yb)h)$, und da folglich $g \cdot \big(\sum_{i\in I} a_i \otimes b_i c\big) = g \cdot \big(\sum_{i\in I} ca_i \otimes b_i\big)$. Damit ist $\tilde{g}$ insgesamt $L \otimes_K F$-linear.

(iv) $\Longleftrightarrow$ (viii). $L \otimes_K K^{p^{-1}}$ ist halbeinfach genau dann, wenn das Jacobson-Radikal verschwindet, und das stimmt für eine kommutative endlichdimensionale $K^{p^{-1}}$-Algebra mit dem Nilradikal, i.e. der Teilmenge aller nilpotenten Elemente, überein.

(viii) $\Longrightarrow$ (ix). Nehmen wir im Gegenteil an, es habe $x \in L$ ein nicht-separables Minimalpolynom $\mu_{x,K}(X)$. Dann ist wegen der mehrfachen Nullstelle in $\bar{K}$ das Ideal $(\mu_{x,K}(X), \mu'_{x,K}(X)) \neq K[X]$, da sonst das Ideal $(\mu_{x,K}(X), \mu'_{x,K}(X)) = \bar{K}[X]$ wäre, was wegen des gemeinsamen Linearfaktors nicht richtig ist. Da $\deg \mu'_{x,K} < \deg \mu_{x,K}$, und da $\mu_{x,K}(X)$ irreduzibel ist, muß notwendig $\mu'_{x,K}(X) = 0$ sein. D.h. wir haben $\mu_{x,K}(X) = \sum_{i\in[0,n]} \alpha_i X^{ip}$ für gewisse $\alpha_i \in K$. Es ist somit $\xi := \sum_{i\in[0,n]} \alpha_i^{p^{-1}} \otimes x^i \neq 0$, da $(x^0, \ldots, x^n)$ linear unabhängig über K wegen $n < np$, aber $\xi^p = 0$.

Nebenbei bemerkt, das Tupel $(x^0, \ldots, x^n)$ ist linear unabhängig über K, nicht aber das Tupel $((x^0)^p, \ldots, (x^n)^p)$, was direkt zeigt, daß (i) nicht gilt, d.h. (i) $\Longrightarrow$ (ix).

(ix) $\Longrightarrow$ (x). Wir finden ein primitives Element $x \in L$, i.e. $L = K(x)$. Es hat $\mu_{x,K}(X)$ insgesamt $n := [L : K]$ paarweise verschiedene Nullstellen $\xi_1, \ldots, \xi_n$ in $\bar{K}$, und entsprechend gibt es n Einbettungen $\sigma_1, \ldots, \sigma_n$ von L nach $\bar{K}$ über K, charakterisiert durch $x \longmapsto \xi_i$. Diese Einbettungen sind linear unabhängig im $\bar{K}$-Vektorraum $\mathrm{Hom}_K(L, \bar{K})$ (Dedekinds Lemma). Es folgt der Isomorphismus

$$\begin{array}{ccccc} L & \otimes_K & \bar{K} & \xrightarrow{\sim} & \prod_{i\in[1,n]} \bar{K} \\ x & \otimes & y & \longmapsto & ((x\sigma_i)y)_{i\in[1,n]}\,, \end{array}$$

da mit der linearen Unabhängigkeit der Spalten einer beschreibenden $\bar{K}$-linearen Matrix $(x_i\sigma_j)_{i,j}$ selbige Rang n hat.

(x) $\Longrightarrow$ (xi). Wäre $\mathrm{Tr}_{L|K} = 0$, so auch $\bar{K} \otimes_K \mathrm{Tr}_{L|K}$, und mit (x) also auch $\mathrm{Tr}_{(\prod_{i\in I} \bar{K})|\bar{K}} = 0$, was nicht der Fall ist wegen $\mathrm{Tr}_{(\prod_{i\in I} \bar{K})|\bar{K}}(1, 0, \ldots, 0) = 1$.

(xi) $\Longrightarrow$ (ix). Wir nehmen an, daß (ix) nicht gilt, daß es also ein Element $x \in L$ mit $\mu_{x,K}(X) = f(X^{p^s})$ für ein $f(X) \in K[X]$ irreduzibel mit $f'(X) \neq 0$ und $s \geq 1$ gibt (vgl. Beweis zu (viii) $\Longrightarrow$ (ix)). Dann ist $y := x^{p^s}$ separabel über K, da $f(X)$ separabel und $f(y) = 0$. Da $f(X)$ irreduzibel ist, ist darüberhinaus $\mu_{y,K}(X) = f(X)$.

Wir haben die Zwischenerweiterung $L|K(x)|K(y)|K$, mit $[K(x):K(y)] = [K(x):K]/[K(y):K] = p^s$, und folglich $\mu_{x,K(y)}(X) = X^{p^s} - y$. Es ist nun $\mathrm{Tr}_{K(x)|K(y)}(x^i) = 0$ für alle $i \in [0, p^s - 1]$, wie man anhand der Basis $(x^0, \ldots, x^{p^s-1})$ nachprüft, und somit $\mathrm{Tr}_{K(y)|K(x)} = 0$. Daher ist auch $\mathrm{Tr}_{L|K} = \mathrm{Tr}_{K(x)|K} \circ \mathrm{Tr}_{K(y)|K(x)} \circ \mathrm{Tr}_{L|K(y)} = 0$.

(x) $\Longrightarrow$ (v). Wäre $L \otimes_K F$ nicht halbeinfach, so enthielte sie ein nilpotentes Element ungleich 0, und das träfe dann auch für $L \otimes_K \bar{K} \supseteq L \otimes_K F$ zu. Mit (x) ist das aber nicht der Fall.

(3) Sei $\mathbf{F}_4 = \mathbf{F}_2(\alpha)$ mit $\alpha^2 + \alpha + 1 = 0$. Es ist $\mathbf{F}_4|\mathbf{F}_2$ separabel (was auch mit (1) folgt). Im einzelnen erhalten wir das folgende.

  (i) Für Tupel aus einem oder keinem Element ist die behauptete lineare Unabhängigkeit klar. Sei nun $(u\alpha + v, u'\alpha + v')$ linear unabhängig über $\mathbf{F}_2$, i.e. sei $uv' \neq u'v$. Dann ist auch $((u\alpha + v)^2, (u'\alpha + v')^2) = (u\alpha^2 + v, u'\alpha^2 + v')$ linear unabhängig über $\mathbf{F}_2$, da $(\alpha^2, 1) = (\alpha + 1, 1)$ linear unabhängig ist, und da weiterhin $uv' \neq u'v$.

  (vi) Es genügt, eine $\mathbf{F}_4$-$\mathbf{F}_4$-lineare Aufspaltung des Multiplikationsepimorphismus $\mathbf{F}_4 \otimes_{\mathbf{F}_2} \mathbf{F}_4 \longrightarrow \mathbf{F}_4$ anzugeben. Unter Zuhilfenahme von $\mathbf{F}_4 \otimes_{\mathbf{F}_2} \mathbf{F}_4 \xrightarrow{\sim} \mathbf{F}_4 \times \mathbf{F}_4$ erhält man die durch $1 \longmapsto 1 \otimes 1 + 1 \otimes \alpha + \alpha \otimes 1$ festgelegte Abbildung.

  (ix) Die Elemente $0, 1$ haben sicher separable Minimalpolynome über $\mathbf{F}_2$. Die Elemente α und $\alpha^2 = \alpha + 1$ sind die beiden verschiedenen Nullstellen des irreduziblen Polynoms $f(X) = X^2 + X + 1$. Man sieht auch, daß $f'(X) = 1$ nicht verschwindet.

  (x) Via $1 \otimes 1 \longmapsto (1,1)$ und $\alpha \otimes 1 \longmapsto (\alpha, \alpha^2)$ wird bereits $\mathbf{F}_4 \otimes_{\mathbf{F}_2} \mathbf{F}_4 \xrightarrow{\sim} \mathbf{F}_4 \times \mathbf{F}_4$, da die $\mathbf{F}_4$-lineare beschreibende Matrix $\left(\begin{smallmatrix} 1 & 1 \\ \alpha & \alpha^2 \end{smallmatrix}\right)$ Determinante 1 hat. Sieht man $\mathbf{F}_4 \subseteq \bar{\mathbf{F}}_2$ und tensoriert diesen Isomorphismus noch mit $- \otimes_{\mathbf{F}_4} \bar{\mathbf{F}}_2$, so erhält man den gewünschten Isomorphismus.

  (xi) In der Tat ist $\mathrm{Tr}_{\mathbf{F}_4|\mathbf{F}_2}(\alpha) = \alpha + \alpha^2 = 1$.

(4) Es ist $(\mathbf{F}_p(X^{p^{-1}}))\mathrm{F} = \mathbf{F}_p(X)$ (als Teilmengen von $\overline{\mathbf{F}_p(X)}$), und also auch $\mathbf{F}_p(X^{p^{-1}}) = (\mathbf{F}_p(X))\mathrm{F}^{-1}$. Es ist $\mathbf{F}_p(X^{p^{-1}})|\mathbf{F}_p(X)$ nicht separabel. Im einzelnen erhalten wir das folgende.

  (i) Es ist $(1, X^{p^{-1}})$ linear unabhängig über $\mathbf{F}_p(X)$, nicht aber $(1, X)$.

  (vi) Wir wollen zeigen, daß der $\mathbf{F}_p(X^{p^{-1}}) \otimes_{\mathbf{F}_p(X)} \mathbf{F}_p(X^{p^{-1}})$-Modul $\mathbf{F}_p(X^{p^{-1}})$ nicht projektiv ist. Wegen $\mathbf{F}_p(X^{p^{-1}}) \otimes_{\mathbf{F}_p(X)} \mathbf{F}_p(X^{p^{-1}}) \simeq \mathbf{F}_p(X^{p^{-1}})[Z]/(Z^p)$ (cf. ix) können wir dazu zeigen, daß allgemein für K ein Körper und $m \geq 2$ der $K[Z]/(Z^m)$-Modul K, auf dem Z wie 0 operiert, nicht projektiv ist. In der Tat spaltet der Epimorphismus $K[Z]/(Z^m) \longrightarrow K$, $Z \longmapsto 0$, nicht auf. Wäre nämlich ξ das Bild von $1 \in K$, so müßte $Z\xi = 0$ sein, i.e. $\xi \in (Z^{m-1}) \subseteq (Z)$. Damit liegt ξ im Kern unserer Abbildung, kann also insbesondere nicht auf 1 gehen.

  (ix) Es ist

$$\begin{array}{rcl} \mathbf{F}_p(X^{p^{-1}}) \otimes_{\mathbf{F}_p(X)} \overline{\mathbf{F}_p(X)} & \simeq & \overline{\mathbf{F}_p(X)}[Y]/(Y^p - X) \\ & = & \overline{\mathbf{F}_p(X)}[Y]/(Y - X^{p^{-1}})^p \\ & \simeq & \overline{\mathbf{F}_p(X)}[Z]/(Z)^p \,, \end{array}$$

das Tensorprodukt enthält also das zu Z, i.e. zu $Y - X^{p^{-1}}$ korrespondierende nilpotente Element $X^{p^{-1}} \otimes 1 - 1 \otimes X^{p^{-1}} \neq 0$. Ein endliches direktes Produkt von Kopien von $\overline{\mathbf{F}_p(X)}$ enthält aber keine nilpotenten Elemente ungleich 0, und somit existiert kein Isomorphismus der fraglichen Form.

(xi) Bezüglich der Basis $((X^{p^{-1}})^0, \dots, (X^{p^{-1}})^{p-1})$ sieht man, daß $\mathrm{Tr}_{\mathbf{F}_p(X^{p^{-1}})|\mathbf{F}_p(X)} = 0$ (vgl. Beweis zu (2), (xi) $\Longrightarrow$ (ix)).

(5) Sei $(f_1(X), \dots, f_m(X))$ ein über K linear unabhängiges Tupel in $K(X)$. Da die lineare Unabhängigkeit eines Tupels sich bei Multiplikation mit einem festen Element in $K(X)$ nicht ändert, weder von $(f_i(X))_i$ noch von $(f_i(X)^p)_i$, dürfen wir annehmen, daß $f_i(X) = \sum_{j \in [1,k]} a_{i,j} X^j \in K[X]$ für $i \in [1, m]$. Sei nun $\sum_i \lambda_i f_i(X)^p = 0$ mit $\lambda_i \in K$, i.e. $\sum_i \lambda_i a_{i,j}^p = 0$ für alle $j \in [1, k]$. Wäre ein $\lambda_i \neq 0$, so wäre die Matrix $(a_{i,j}^p)_{i \in [1,m], j \in [1,k]}$ von Rang $< m$. Also wären alle $m \times m$-Unterdeterminanten von $(a_{i,j}^p)_{i,j}$ gleich 0. Eine solche Unterdeterminante ist aber gerade die p-Potenz der entsprechenden Unterdeterminante von $(a_{i,j})_{i,j}$, und von denen verschwindet eine nach Voraussetzung nicht. (Oder: Der Rang einer Matrix ändert sich beim Übergang nach $\bar{K}$ nicht. Wende eintragsweise F^{-1} darauf an, unter Automorphismen ändert sich der Rang auch nicht. Also muß der Rang gleich m gewesen sein.) Damit ist auch das Tupel $(f_i(X)^p)_i$ linear unabhängig über K, und somit $K(X)|K$ separabel.