

Aufgabe	A1	A2	A3	A4	Σ
Punkte					

Aufgabe 1. Beh.: K vollkommen $\iff (f \in K[X] \text{ irreduzibel} \implies f \text{ separabel})$.

Beweis. • „ $\implies$ “: Sei K vollkommen und $f \in K[X]$ irreduzibel und $\alpha \in \overline{K}$ mit $\overline{K}$ ein algebraischer Abschluss von K . Dann betrachte $L := K(\alpha)$. L ist separabel über K , da K vollkommen, insbesondere α separabel über K , also f , Minimalpolynom von α , separabel über K .

- „ $\impliedby$ “: Sei L/K algebraische Körpererweiterung und $\alpha \in L$. Dann sei $f \in K[X]$ Minimalpolynom von α über K . Dann ist f irreduzibel, also separabel und damit α separabel und damit L/K separabel. Da L beliebig, folgt K vollkommen.

Beh.: σ surjektiv $\iff K$ vollkommen.

Beweis. • „ $\implies$ “: Sei σ surjektiv und $f \in K[X]$ irreduzibel. Mit der Vorüberlegung genügt es zu zeigen, dass f separabel ist. Da $\text{char}(K) = p > 0$ sei $r \in \mathbb{N}_0$ maximal, s.d. $f(X) = g(X^{p^r})$ für ein $g \in K[X]$. Dann hat nach VL jede Nullstelle von f Vielfachheit p^r . Ang.: $r > 0$. Dann ex. insbesondere ein $f(X) = h(X^p)$ für $h \in K[X]$. Dann ex. $a_i \in K$ und da σ surjektiv, $\alpha_i \in K$, s.d. $a_i = \alpha_i^p \forall i$. Damit folgt

$$f = \sum_{i=1}^n a_i X^{ip} = \sum_{i=1}^n \alpha_i^p (X^i)^p = \left(\sum_{i=1}^n \alpha_i X^i \right)^p.$$

Also ist f reduzibel $\nmid$. Damit folgt $r = 0$, also hat jede Nullstelle von f genau Vielfachheit 1, insbesondere f separabel.

- „ $\impliedby$ “: Sei K vollkommen und $a \in K$. Dann betrachte $f := X^p - a$. Sei $\alpha \in \overline{K}$ mit $\overline{K}$ ein algebraischer Abschluss von K Nullstelle von f . Dann folgt $\alpha^p = a$. Damit folgt da $\text{char}(K) = p > 0$:

$$(X - \alpha)^p = X^p - \alpha^p = X^p - a = f.$$

Also ist α Nullstelle von f mit p -facher Vielfachheit. Also f nicht separabel und mit der Vorüberlegung also f reduzibel über K . Sei $g \in K[X]$ ein irreduzibler Faktor von f mit $\deg(g) = r$. Dann ist α Nullstelle von g mit r -facher Vielfachheit und da g irreduzibel, ist g separabel nach der Vorüberlegung. Also folgt $r = 1$ und $g = X - \alpha \in K[X]$. Insbesondere folgt $\alpha \in K$ und wegen $\alpha^p = a$ folgt σ surjektiv.

□

□

Aufgabe 2. (a) Beh.: Ist K vollkommen, so auch L .

Beweis. Sei M/L eine algebraische Körpererweiterung. Da M/L und L/K algebraisch, ist auch M/K algebraisch und da K vollkommen damit M/K separabel. Also insbesondere M/L separabel. Da M/L beliebig, folgt L vollkommen. □

(b) Beh.: L/K separabel $\implies K$ vollkommen.

Beweis. Sei M/K algebraische Körpererweiterung und sei $\alpha \in M$ beliebig. Betrachte das Kompositum $E := K(\alpha)L$. Es ist E/L endliche algebraische Erweiterung, da $K(\alpha)/K$ und L/K endlich und algebraisch. Da L vollkommen, ist also E/L separabel. Da außerdem L/K separabel, ist auch E/K separabel. Insbesondere ist also $\alpha \in K(\alpha) \subseteq E$ separabel über K . Da α beliebig, folgt M/K separabel. □

(c) Beh.: L/K separabel.

Beweis. Setze $n := [L : K] < \infty$. Dann sei $\alpha \in L$ und $f \in K[X]$ Minimalpolynom zu α . Da $\text{char}(K) = p > 0$ sei $r \in \mathbb{N}_0$ maximal, s.d. $f(X) = g(X^{p^r})$ für ein $g \in K[X]$. Da f irreduzibel ist g nach VL separabel und $f(\alpha) = 0 \implies g(\alpha^{p^r}) = 0$. Also α^{p^r} Nullstelle eines separablen Polynoms über K , also separabel über K . Es folgt also $\alpha^{p^r} \in K_s$. Ang.: $r > n$. Da

$$n = [L : K] = [L : K(\alpha)][K(\alpha) : K] = [L : K(\alpha)]\deg(f),$$

folgt $\deg(f) \leq n$. Also insbesondere $r > \deg(f)$. Dann

$$\deg(f) = \underbrace{\deg(g)}_{\geq 1} p^r > p^r > p^n > \deg(f) \quad \text{!}$$

Also folgt $r \leq n$. Damit folgt da K_s Körper

$$\alpha^{p^n} = \alpha^{p^{n-r} p^r} = (\alpha^{p^r})^{p^{n-r}} \in K_s.$$

Sei nun $a \in L$. Da L vollkommen, ist nach Aufgabe 1 σ bijektiv, damit ist auch $\sigma^n: L \rightarrow L, x \mapsto \sigma(x)^n = x^{p^n}$ bijektiv als Komposition bijektiver Abbildungen. Also ex. ein $\alpha \in L$, s.d. $\sigma^n(\alpha) = a$. Also folgt mit der Vorüberlegung $a = \alpha^{p^n} \in K_s$, also a separabel über K und damit L/K separabel. $\square$

Aufgabe 3. (a) Beh.: Jede quadratische Erweiterung L ist von der Form $L = K(\sqrt{a})$ für ein $a \in K^\times \setminus (K^\times)^2$.

Beweis. Sei L/K quadratische Erweiterung. Dann ist $[L : K] = 2$ insbesondere algebraisch und endlich. Also $L = K(\alpha_1, \dots, \alpha_n)$ für $\alpha_1, \dots, \alpha_n \in L$. Da der Grad von echten Erweiterungen echt größer als 1 ist, folgt mit Gradformel $L = K(\alpha)$ für ein $\alpha \in L$ mit Minimalpolynom

$$f = X^2 + \tilde{b}X + c$$

für $b, c \in K$. Da $\text{char}(K) \neq 2 \implies \exists b \in K$, s.d. $2b = \tilde{b}$. Damit ist

$$f = X^2 + 2bX + c.$$

Da $f(\alpha) = 0$ folgt

$$\alpha^2 + 2b\alpha + c = \alpha^2 + 2b\alpha + b^2 - b^2 + c = (\alpha + b)^2 + c - b^2 = 0.$$

Also insbesondere

$$(\alpha + b)^2 = b^2 - c$$

und damit $\alpha \in K(\sqrt{b^2 - c})$. Also $K(\alpha) \subseteq K(\sqrt{b^2 - c})$. Außerdem gilt für $g := X^2 - b^2 + c$: $g(\sqrt{b^2 - c}) = 0$, also $[K(\sqrt{b^2 - c}) : K] \leq 2$. Also folgt mit Gradformel

$$2 \geq [K(\sqrt{b^2 - c} : K) = [K(\sqrt{b^2 - c}) : K(\alpha)][K(\alpha) : K] = 2[K(\sqrt{b^2 - c}) : K(\alpha)].$$

Damit folgt $[K(\sqrt{b^2 - c}) : K(\alpha)] = 1$ also $K(\alpha) = K(\sqrt{b^2 - c})$.

Es ist $b^2 - c \neq 0$, denn sonst $\alpha = -b \in K$, also $L = K$. Ang.: $b^2 - c \in (K^\times)^2$, dann ist $\sqrt{b^2 - c} \in K^\times$, also insbesondere $K(\alpha) = K$ also $[L : K] = 1 \neq 2$!

Also folgt $L = K(\sqrt{b^2 - c})$ und $b^2 - c \in K^\times \setminus (K^\times)^2$. $\square$

(b) Beh.: Zwei Erweiterungen $K(\sqrt{a})$ und $K(\sqrt{b})$ mit $a, b \in K^\times$ sind genau dann K -isomorph, wenn $\frac{a}{b} \in (K^\times)^2$.

Beweis. • „ $\implies$ “: Sei $\varphi: K(\sqrt{a}) \rightarrow K(\sqrt{b})$ K -Isomorphismus. Dann $\exists x \in K(\sqrt{a})$, s.d. $\varphi(x) = \sqrt{b}$. Da φ K -Iso folgt außerdem $\varphi(b) = b$. Also folgt damit

$$\varphi(x^2) = \varphi(x)^2 = b = \varphi(b).$$

Da φ injektiv, folgt $x^2 = b$. Also insbesondere $\sqrt{b} \in K(\sqrt{a})$.

Falls $K(\sqrt{a}) = K$, dann ist $\sqrt{a}, \sqrt{b} \in K^\times$, da $a, b \in K^\times$, insbesondere $\frac{a}{b} \in (K^\times)^2$.

Sei nun $K(\sqrt{a}) \neq K$. Da $\sqrt{b} \in K(\sqrt{a})$ ex. $u, v \in K$, s.d. $\sqrt{b} = u + v\sqrt{a}$.

Ang.: $v = 0$, dann ist $\sqrt{b} \in K$, also $K(\sqrt{b}) = K$ und da φ K -Isomorphismus auch $K(\sqrt{a}) = K$ ∇ .

Ang.: $u \neq 0$: Dann gilt wegen $\text{char}(K) \neq 2$:

$$b = (u + v\sqrt{a})^2 = u^2 + 2uv\sqrt{a} + a \implies \sqrt{a} = \frac{b - u^2 - a}{2uv} \in K.$$

Also $\sqrt{a} \in K$, also insbesondere $K(\sqrt{a}) = K$ ∇ .

Also folgt $\sqrt{b} = v\sqrt{a}$, also $\sqrt{\frac{a}{b}} = \frac{1}{v} \in K$, also da $a, b \in K^\times$ auch $\frac{a}{b} \in (K^\times)^2$.

- „ $\Leftarrow$ “: Es sei $\sqrt{\frac{a}{b}} \in K$. Dann ist

$$K(\sqrt{a}) = K\left(\sqrt{\frac{a}{b}b}\right) = K\left(\sqrt{\frac{a}{b}}\sqrt{b}\right) \cong K(\sqrt{b}).$$

□

(c) Beh.: Für p ungerade Primzahl und $a \in \mathbb{F}_p^\times$ gilt

$$a^{\frac{p-1}{2}} = \begin{cases} 1 & a \in (\mathbb{F}_p^\times)^2 \\ -1 & a \notin (\mathbb{F}_p^\times)^2 \end{cases}.$$

Beweis. Es ist zunächst $\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} = 1$, da $\text{ord}(\mathbb{F}_p^\times) = p-1$ und kl. Satz v. Fermat. Damit folgt

$$\left(a^{\frac{p-1}{2}}\right)^2 - 1 = 0 \implies \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) = 0.$$

Da $\mathbb{F}_p$ nullteilerfrei, folgt $a^{\frac{p-1}{2}} = 1$ oder $a^{\frac{p-1}{2}} = -1$. Es genügt also zu zeigen, dass $a^{\frac{p-1}{2}} = 1 \iff a \in (\mathbb{F}_p^\times)^2$.

- „ $\implies$ “: Sei $a \in (\mathbb{F}_p^\times)^2$. Dann ex. ein $x \in \mathbb{F}_p^\times$ mit $x^2 = a$. Damit folgt wieder mit Satz v. Fermat

$$a^{\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} = x^{p-1} = 1.$$

- „ $\Leftarrow$ “: Sei $a^{\frac{p-1}{2}} = 1$. Es ist $\mathbb{F}_p^\times$ zyklisch, also ex. ein $x \in \mathbb{F}_p^\times$ und ein $r \in \mathbb{N}$, s.d. $x^r = a$. Dann folgt

$$1 = a^{\frac{p-1}{2}} = (x^r)^{\frac{p-1}{2}} = x^{r\frac{p-1}{2}}.$$

Da $\text{ord}(x) = p-1$ folgt $(p-1) \mid r\frac{p-1}{2}$. Also folgt $\frac{r}{2} \in \mathbb{N}$ also r gerade. Damit $\exists k \in \mathbb{N}$, s.d. $r = 2k$. Damit folgt

$$a = x^r = x^{2k} = \underbrace{(x^k)^2}_{\in \mathbb{F}_p^\times}.$$

Also $a \in (\mathbb{F}_p^\times)^2$.

□

Aufgabe 4. (a) Beh.: $f \in \mathbb{F}_p[X]$ irreduzibel: $f \mid (X^{p^n} - X) \iff \deg(f) \mid n$.

Beweis. Sei $f \in K[X]$ irreduzibel.

- „ $\implies$ “: Es sei $f \mid (X^{p^n} - X)$. Es zerfällt $X^{p^n} - X$ über $\mathbb{F}_{p^n}$ in Linearfaktoren und da $f \mid (X^{p^n} - X)$ zerfällt auch f über $\mathbb{F}_{p^n}$ in Linearfaktoren.

Sei $\alpha \in \mathbb{F}_{p^n}$ eine Nullstelle von f . Dann ist α auch Nullstelle von $X^{p^n} - X$ und da $\mathbb{F}_{p^n}$ gerade von diesen Nullstellen erzeugt, folgt $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}$. Außerdem ist f irreduzibel, also gerade das Minimalpolynom von α über $\mathbb{F}_p$. Damit folgt mit Gradformel

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p(\alpha)][\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p(\alpha)]\deg(f).$$

Damit folgt $\deg(f) \mid n$.

- „ $\Leftarrow$ “: Es sei $\deg(f) \mid n$. Dann betrachte $K := \mathbb{F}_p(X)/(f)$. Da $\mathbb{F}_p$ Körper, ist $\mathbb{F}_p[X]$ HIR und da f irreduzibel ist also K Körper. Falls $f = X$, dann ist $X \mid (X^{p^n} - X)$. Sei also $f \neq X$. Es ist $\dim_{\mathbb{F}_p} K = \deg(f) =: d$ nach Zettel 3, da $f \neq 0$, da f irreduzibel. Da $\#\mathbb{F}_p = p$ folgt $\#K = p^d$. Da $f \neq X$ folgt $f \nmid X$, denn f irreduzibel und damit $d \geq 1$. Also ist $X \in K^\times$ und damit mit Satz von Fermat: $X^{p^d} = X$ in K . Damit folgt $X^{p^d} - X \in (f)$. Da nun $d \mid n$ ex. ein $q \in \mathbb{N}$, s.d. $n = qd$. Damit folgt $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^{dq}} = \mathbb{F}_{p^n}$, also sind Nullstellen von $X^{p^d} - X$ auch Nullstellen von $X^{p^n} - X$ (da $\mathbb{F}_{p^d}$ bzw. $\mathbb{F}_{p^n}$ Zerfällungskörper über diese Polynome), also $(X^{p^d} - X) \mid (X^{p^n} - X)$. Insgesamt folgt also $f \mid (X^{p^n} - X)$.

□

(b) Beh.:

$$X^{p^n} - X = \prod_f f(X)$$

wobei f die irreduziblen normierten Polynome in $\mathbb{F}_p[X]$ mit $\deg(f) \mid n$ durchlaufen.

Beweis. Die Teiler von $X^{p^n} - X$ sind wegen (a) genau die irreduziblen Polynome $f \in K[X]$ mit $\deg(f) \mid n$. Da $X^{p^n} - X$ normiert können diese normiert gewählt werden. Da außerdem $X^{p^n} - X$ separabel über $\mathbb{F}_p$, sind die normierten Teiler von $X^{p^n} - X$ paarweise verschieden. Das zeigt die Behauptung. □

(c) Beh.: $\sum_{d \mid n} da_d(p) = p^n$

Beweis. Es ist für $d \in \mathbb{N}$ und f durchlaufe die normierten irreduziblen Polynome gilt

$$\sum_{\deg(f)=d} \deg(f) = da_d(p).$$

Damit folgt wenn $f \in \mathbb{F}_p[X]$ wieder die normierten irreduziblen Polynome mit $\deg(f) \mid n$ durchläuft mit Umordnung der vorletzten Summe und der Vorüberlegung:

$$p^n = \deg(X^{p^n} - X) \stackrel{(b)}{=} \sum_f \deg(f) = \sum_{d \mid n} da_d(p).$$

□

(d) Beh.: $a_6(2) = 9$.

Beweis. Es genügt die positiven Teiler zu betrachten, da $\deg(f) \geq 1$ für $f \in \mathbb{F}_p[X]$ irreduzibel. Damit folgt mit Anwendung von (c):

$$(i) \text{ 1 hat Teiler 1, also } 2^1 = 1 \cdot a_1(2) \implies a_1(2) = 2.$$

$$(ii) \text{ 2 hat Teiler 1 und 2, also } 2^2 = a_1(2) + 2a_2(2) \implies a_2(2) = 1.$$

$$(iii) \text{ 3 hat Teiler 1 und 3, also } 2^3 = a_1(2) + 3a_3(2) \implies a_3(2) = 2.$$

6 hat Teiler 1, 2, 3 und 6. Damit folgt

$$2^6 = a_1(2) + 2a_2(2) + 3a_3(2) + 6a_6(2) \implies a_6(2) = 9.$$

□