Aufgabe 1

Sei K vollkommen. Angenommen, σ wäre nicht surjektiv. Dann gäbe es ein $a \in K$ derart, dass $X^p - a$ keine Nullstelle in K besitzt. Sei nun $\alpha \in \overline{K}$ eine Nullstelle von $X^p - a$, d.h. $\alpha^p = a$. Damit gilt $X^p - a = X^p - \alpha^p = (X-\alpha)^p$. Wäre $X^p - a$ reduzibel über K, so müsste es in Faktoren der Form $X^p - a = (X-\alpha)^r \cdot (X-\alpha)^{p-r}$. Ein Polynom der Form $(X-\alpha)^r$ kann aber nicht in K liegen. Für $r = 1$ würde $\alpha \in K$ folgen. Für $1 < r < p$ gilt $(X-\alpha)^r = \sum_{i=1}^{r} \binom{r}{i}(-\alpha)^i X^{r-i} \in K[X]$. Der Koeffizient vor X^{r-1} ist $\binom{r}{1}(-\alpha)^1 = -r\alpha$. Es gilt aber $-r\alpha \in K \implies \alpha \in K$. Das ist ein Widerspruch. Das Polynom $X^p - a$ ist also irreduzibel in K und damit Minimalpolynom zu α. Allerdings hat $X^p - a$ die Mehrfachnullstelle α, $X^p - a = (X-\alpha)^p$. Daher ist α nicht separabel. Das ist ein Widerspruch zur Vollkommenheit von K. Daher muss σ surjektiv sein. Sei nun σ surjektiv und f ein irreduzibles Polynom in $K[X]$. Wir nehmen nun an, dass f eine Mehrfachnullstelle besitzt. Nach Satz 3.81 ist f dann ein Polynom in X^p. Es gilt also

$$f = a_n(X^p)^n + a_{n-1}(X^p)^{n-1} + \cdots + a_0 = a_n X^{p\cdot n} + a_{n-1}X^{p\cdot(n-1)} + \cdots + a_0$$

Da σ surjektiv ist, existiert zu jedem a_i ein c_i mit $c_i^p = a_i$. Wir erhalten also

$$f = c_n^p(X^n)^p + c_{n-1}^p(X^{n-1})^p + \cdots + c_0^p = (c_nX^n + c_{n-1}X^{n-1})^p + \cdots + c_0^p = (c_nX^n + c_{n-1}X^{n-1} + \cdots + c_0)^p$$

wobei die letzte Gleichheit induktiv sofort klar ist. Das ist aber ein Widerspruch zur Irreduzibilität von f. Also kann f keine Mehrfachnullstelle besitzen, jedes irreduzible Polynom über K ist separabel. Da $\forall \alpha \in \overline{K}$ das Minimalpolynom irreduzibel ist, sind alle $\alpha \in \overline{K}$ separabel und folglich ist jede algebraische Körpererweiterung separabel.

Aufgabe 2

(a) Sei M/L eine beliebige Körpererweiterung. Dann wird M durch M/L und L/K zu einer Erweiterung M/K von K. Aufgrund der Vollkommenheit von K ist M/K separabel. Nach Lemma 3.93 ist demnach auch M/L separabel. Weil M beliebig gewählt war ist damit die Vollkommenheit von L gezeigt.

(b) Wegen $L \subset \overline{K}$ ist die Erweiterung $\overline{K}/L$ separabel. Sind die Erweiterungen $\overline{K}/L$ und L/K separabel, so auch $\overline{K}/K$. Sei M eine algebraische Erweiterung von K. Dann sind nach Korollar 3.93 $\overline{K}/M$ und M/K separabel. Also ist jede algebraische Erweiterung von K separabel und damit K vollkommen.

(c) Sei $x \in K_s \subset L$. Dann ist $x^{p^n} \in K_s$, da K_s ein Körper ist. Sei nun $x \in L \setminus K_s$. Dann ist das Minimalpolynom f von x über K nicht separabel und nach Lemma 3.81 existiert ein $r \in \mathbb{N}$ (also $r \neq 0$) mit $f(X) = g(X^r)$, wobei g irreduzibel und separabel ist. Wegen $f(x) = 0$ muss auch $g(x^r) = 0$ sein. Daher ist g das Minimalpolynom zu x^r und x^r muss separabel sein. Daher existiert für alle $x \in L$ ein $r \in \mathbb{N}$ derart, dass $x^{p^n} \in K_s \forall n \geq r$. Aufgrund der Endlichkeit von L/K ist aber der Grad eines Minimalpolynoms beschränkt. Es existiert daher ein $n \in \mathbb{N}$ derart, dass $\forall x \in L\colon\ x^{p^n} \in K_s$. Da L vollkommen ist, muss der Frobenius-Homomorphismus $\sigma\colon L \to L, a \mapsto a^p$ bijektiv sein. Insbesondere existiert daher für alle $x \in L$ ein $\tilde{x}$ mit $x = \sigma^n(\tilde{x}) = (\tilde{x})^{p^n} \in K_s$. Daher ist L/K separabel.

Aufgabe 3

(a) Eine quadratische Erweiterung wird stets von einem Element α erzeugt, da es keine Teilerweiterungen gibt. Das Minimalpolynom zu α ist ein irreduzibles Polynom vom Grad 2 und hat daher die Form $f(X) = X^2 + pX + q$, das eine Nullstelle bei α hat. Jede Nullstelle von f hat die Form $\alpha = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$. Daher ist also $K(\alpha) = K(-\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}) = K(\sqrt{\left(\frac{p}{2}\right)^2 - q})$. Wäre $\left(\frac{p}{2}\right)^2 - q = 0$, so zerfiele f in Linearfaktoren $f(X) = (X + \frac{p}{2})^2$ und folglich nicht irreduzibel. Wäre $\left(\frac{p}{2}\right)^2 - q = a^2$ für ein $a \in K^\times$, so wäre $f(X) = (X + \frac{p}{2} + a)(X + \frac{p}{2} - a)$ und folglich nicht irreduzibel. Daher muss $a \in K^\times \setminus (K^\times)^2$ liegen.

(b) Sei $c^2 = \frac{a}{b}$ mit $c \in K^\times$. Dann gilt $\sqrt{a} = \sqrt{b \cdot \frac{a}{b}} = \sqrt{b} \cdot \sqrt{\frac{a}{b}} = c \cdot \sqrt{b} \in K(\sqrt{a}) \implies K(\sqrt{b}) \subset K(\sqrt{a})$. Analog erhält man die Umkehrung, sodass folgt $K(\sqrt{a}) = K(\sqrt{b})$. Nach Lemma 3.40 existiert ein K-Isomorphismus zwischen $K(\sqrt{a})$ und $K(\sqrt{b})$ dann, wenn eine Nullstelle des Minimalpolynoms von $\sqrt{a}$ bereits $K(\sqrt{b})$ erzeugt. Das Minimalpolynom von $\sqrt{a}$ ist $X^2 - a$ und hat die beiden Nullstellen $\sqrt{a}$ und $-\sqrt{a}$. Damit muss $K(\sqrt{a}) = K(\sqrt{b})$ und insbesondere $\sqrt{b} \in K(\sqrt{a})$ gelten, wenn ein Isomorphismus existiert. Wegen $\dim_K K(\sqrt{a}) = 2$ und weil $1, \sqrt{a}$ K-linear unabhängig sind (sonst wäre $\sqrt{a} \in K$) lässt sich $\sqrt{b}$ als Linearkombination $\sqrt{b} = c + d\sqrt{a}$ schreiben. Ist nun $c \neq 0$, so folgt daraus $b = c^2 + 2cd\sqrt{a} + d^2 a \implies \sqrt{a} = \frac{b - c^2 - d^2 a}{2cd}$ und damit $\sqrt{a} \in K \lightning$. Also gilt $\sqrt{b} = d\sqrt{a}$. Daraus erhalten wir sofort $\frac{a}{b} = \left(\frac{1}{d}\right)^2 \implies \frac{a}{b} \in (K^\times)^2$.

(c) Ist $a \in (\mathbb{F}_p^\times)^2$, so existiert ein $c \in \mathbb{F}_p^\times$ mit $c^2 = a$. Dann ist $a^{\frac{p-1}{2}} = c^{p-1}$. Wegen $c^p = c$ und $c \in K^\times$ ist $a^{\frac{p-1}{2}} = c^{p-1} = 1$. Ist a hingegen in $(\mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2)$, so gilt $(a^{\frac{p-1}{2}})^2 = 1$ durch analoge Rechnung wie im ersten Fall, also $a^{\frac{p-1}{2}} = \pm 1$. Da $\mathbb{F}_p^\times$ nach Vorlesung zyklisch ist, existiert ein $a \in \mathbb{F}_p^\times$ mit $\mathbb{F}_p^\times = \{a, a^2, \ldots, a^{p-1}\}$. Wäre nun $a^{\frac{p-1}{2}} = 1$, so wäre $\#\mathbb{F}_p^\times < p - 1$. Also gilt $a^{\frac{p-1}{2}} = -1$. Für eine ungerade Potenz x von a (z.B. $x = a^3$ gilt offensichtlich ebenfalls $x^{\frac{p-1}{2}} = -1$. Da $(K^\times)^2$ eine Untergruppe vom Index 2 in $\mathbb{F}_p^\times$ bildet und alle geraden Potenzen von a in $(\mathbb{F}_p^\times)^2$ liegen, entsprechen die ungeraden Potenzen von a gerade $\mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2$ und es muss gelten

$$\forall a \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2 \colon a^{\frac{p-1}{2}} = -1.$$

Seien $K(\sqrt{a}), K(\sqrt{b})$ zwei quadratische Erweiterungen von $\mathbb{F}_p$ mit $a, \in K^\times \setminus (K^\times)^2$ und $K(\sqrt{a}) \neq K(\sqrt{b})$, was nach Teilaufgabe b zu $\frac{a}{b} \notin (K^\times)^2$ äquivalent ist. Es gilt aber $1 = \frac{a^{\frac{p-1}{2}}}{b^{\frac{p-1}{2}}} = \left(\frac{a}{b}\right)^{\frac{p-1}{2}}$ und daher $\frac{a}{b} \in (\mathbb{F}_p^\times)^2$. Das ist aber ein Widerspruch. Also kann es keine zwei verschiedenen quadratischen Erweiterungen geben. Die Menge $K^\times \setminus (K^\times)^2$ ist aber für $p \neq 2$ stets nichtleer (siehe Zettel 4, Aufgabe 5 a). Daher existiert eine eindeutig bestimmte quadratische Erweiterung von $\mathbb{F}_p$.

Aufgabe 4

(a) Sei $f \in \mathbb{F}_p[X]$ ein irreduzibles Polynom vom Grad d. Sei a eine Nullstelle von f. Dann hat die Körpererweiterung $\mathbb{F}_p(a)$ Grad d, da f das Minimalpolynom zu a darstellt. Insbesondere ist $\mathbb{F}_p(a)$ als endlichdimensionaler Vektorraum über einem endlichen Körper endlich. Nach Korollar 3.100 ist $\mathbb{F}_p(a)/\mathbb{F}_p$ aber isomorph zu einer Erweiterung $\mathbb{F}_q/\mathbb{F}_p$ mit $q = p^k$. Allerdings muss $[\mathbb{F}_q \colon \mathbb{F}_p] =$

d und damit $q = p^d$ gelten, da der Grad erhalten bleibt. Mit Korollar 3.101 folgt, dass die Körpererweiterung und damit auch f separabel sein muss. f besitzt also d verschiedene Nullstellen in $\overline{\mathbb{F}_p}$, die wir mit $a_1, \dots, a_d$ bezeichnen. Nach Lemma 3.40 ist die Anzahl der Nullstellen von f in $\mathbb{F}_q$ gleich der Anzahl der $\mathbb{F}_p$-Automorphismen $\sigma\colon \mathbb{F}_q \to \mathbb{F}_q$. Diese Anzahl ist gleich $\#\operatorname{Aut}_{\mathbb{F}_p}(\mathbb{F}_q) = [\mathbb{F}_q\colon \mathbb{F}_p] = d$ nach Satz 3.102. Daher liegen alle Nullstellen $a_1, \dots, a_d$ von f in $\mathbb{F}_q$, $\mathbb{F}_q$ ist der Zerfällungskörper von f. f teilt $g \coloneqq X^{p^n} - X$ genau dann, wenn alle Nullstellen von f auch Nullstellen von g sind. Gilt also $f|g$, so sind alle Nullstellen von f auch Nullstellen von g und der Zerfällungskörper von f ist im Zerfällungskörper von g enthalten, d.h. $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$. Ist hingegen der Zerfällungskörper von f im Zerfällungskörper von g enthalten, so ist liegt jede Nullstellen von f in $\mathbb{F}_{p^n}$. Jedes Element von $\mathbb{F}_{p^n}$ ist nach Satz 3.99 aber Nullstelle von $X^{p^n} - X$. Daher gilt

$$f|g \Leftrightarrow \mathbb{F}_q \subset \mathbb{F}_{p^n} \Leftrightarrow \mathbb{F}_{p^d} \subset \mathbb{F}_{p^n} \overset{3.100}{\Longleftrightarrow} d|n \Leftrightarrow \deg f|n$$

(b) Im euklidischen Ring $\mathbb{F}_p[X]$ existiert eine eindeutige Primfaktorzerlegung. Diese ist genau durch alle irreduziblen (normierten) Teiler von $X^{p^n} - X$ gegeben. Nach Teilaufgabe a ist also

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

wobei f die irreduziblen, normierten Polynome in $\mathbb{F}_p$ mit $\deg(f)|n$ durchlaufe.

(c) In der Produktdarstellung in Aufgabe b addieren sich die Grade der Faktoren auf der rechten Seite zum Grad auf der linken Seite, also p^n. Daher gilt

$$p^n = \sum_{\substack{f \text{ irred.} \\ \deg f|n}} \deg(f) = \sum_{d|n} \sum_{\substack{f \text{ irred.} \\ \deg f = d}} d = \sum_{d|n} d \cdot a_d(p)$$

(d) Setzen wir in Aufgabe c $p = 2$ und $n = 6$, so erhalten wir

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

Nach Aufgabe 3 auf Blatt 2 gilt aber $a_1(2) = 2,\ a_2(2) = 1,\ a_3(2) = 2$. Einsetzen ergibt

$$64 = 2 + 2 + 6 + 6a_6(2) \Leftrightarrow 54 = 6a_6(2) \Leftrightarrow a_6(2) = 9.$$

Bonusaufgabe 5

(a)