Aufgabe 1 (Herbst 2004)**.** Seien p, q verschiedene Primzahlen.

(a) Zeigen Sie, daß die Körper $\mathbb{Q}(\sqrt{p})$ und $\mathbb{Q}(\sqrt{q})$ nicht isomorph sind.

(b) Zeigen Sie, daß der Körper $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ vom Grad 4 über $\mathbb{Q}$ ist.

(c) Bestimmen Sie das Minimalpolynom von $\alpha = \sqrt{p} + \sqrt{q}$.

Lösung. **Zu (a):** Wir haben bereits auf Blatt 14 Aufgabe 1 gesehen, daß für $a, b \in \mathbb{Q}^\times$ die Körper $\mathbb{Q}(\sqrt{a})$ und $\mathbb{Q}(\sqrt{b})$ genau dann isomorph sind, wenn $\frac{a}{b} \in (\mathbb{Q}^\times)^2$. Daraus folgt bereits, daß $\mathbb{Q}(\sqrt{p})$ und $\mathbb{Q}(\sqrt{q})$ nicht isomorph sind. Hier noch ein anderer Beweisweg:
Vorbemerkung: Die Körper $\mathbb{Q}(\sqrt{p})$ und $\mathbb{Q}(\sqrt{q})$ sind quadratisch über $\mathbb{Q}$, also normal über $\mathbb{Q}$. Das Minimalpolynom von $\sqrt{q}$ über $\mathbb{Q}$ ist $m_{\mathbb{Q},\sqrt{q}} = X^2 - q$.
Angenommen es gäbe einen Isomorphismus $\varphi : \mathbb{Q}(\sqrt{q}) \to \mathbb{Q}(\sqrt{p})$. Dieser lässt $\mathbb{Q}$ fest und bildet damit $m_{\mathbb{Q},\sqrt{q}}$ auf sich selbst ab. Da $m_{\mathbb{Q},\sqrt{q}}$ in $\mathbb{Q}(\sqrt{q})$ eine Nullstelle hat, ist dem auch so in $\mathbb{Q}(\sqrt{p})$. Es gibt also $\alpha, \beta \in \mathbb{Q}$ mit $(\alpha + \beta\sqrt{p})^2 = q$. Es muß $\alpha \neq 0$, denn sonst $q = p\beta^2$, also $\beta = \sqrt{\frac{q}{p}} \notin \mathbb{Q}$, Widerspruch. Ebenso $\beta \neq 0$, denn q ist keine Quadrat in $\mathbb{Q}$. Also ist

$$q = (\alpha + \beta\sqrt{p})^2 = \alpha^2 + 2\alpha\beta\sqrt{p} + \beta^2 p$$

das heißt

$$\sqrt{p} = \frac{q - \beta^2 p - \alpha^2}{2\alpha\beta} \in \mathbb{Q}$$

Widerspruch.

Zu (b): Nach (a) ist $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$, also $\mathbb{Q}(\sqrt{p}) \subsetneq \mathbb{Q}(\sqrt{p}, \sqrt{q})$ eine echte Erweiterung. Das Minimalpolynom von $\sqrt{q}$ über $\mathbb{Q}$ ist auch irreduzibel über $\mathbb{Q}(\sqrt{p})$:

$$m_{\mathbb{Q}(\sqrt{p}),\sqrt{q}} = m_{\mathbb{Q},\sqrt{q}} = X^2 - q$$

und $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ ist Zerfällungskörper von $m_{\mathbb{Q}(\sqrt{p}),\sqrt{q}}$ über $\mathbb{Q}(\sqrt{p})$, also $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p}) = \deg(m_{\mathbb{Q}(\sqrt{p}),\sqrt{q}}) = 2$. Nach der Gradformel ist

$$[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})][\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Nebenbemerkung: Die Erweiterung $\mathbb{Q}(\sqrt{p}, \sqrt{q})/\mathbb{Q}$ ist normal, denn $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ ist Zerfällungskörper von $(X^2 - p)(X^2 - q)$.

Zu (c): Wir "raten" das Minimalpolynom durch Rückwärtsrechnen. Einmal quadrieren von α ergibt:

$$\alpha^2 = p + q + 2\sqrt{pq}$$

Umstellen und nochmals quadrieren ergibt:

$$(\alpha^2 - p - q)^2 - 4pq = 0.$$

Also ist α Nullstelle des Polynoms

$$f = (X^2 - p - q)^2 - 4pq = X^4 - 2(p + q)X^2 + (p + q)^2 - 4pq = X^4 - 2(p + q)X^2 + (p - q)^2.$$

Es bleibt zu zeigen, daß dies irreduzibel ist.
Dafür zeigen wir, daß α ein primitives Element von $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ ist. Es ist klar, daß $\alpha \in \mathbb{Q}(\sqrt{p}, \sqrt{q})$, also $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Andererseits ist

$$\sqrt{p} = \frac{1}{2}(\alpha + \frac{p - q}{\alpha})$$
$$\sqrt{q} = \frac{1}{2}(\alpha - \frac{p - q}{\alpha})$$

also $\sqrt{p}, \sqrt{q} \in \mathbb{Q}(\alpha)$, das heißt $\mathbb{Q}(\sqrt{p}, \sqrt{q}) \subset \mathbb{Q}(\alpha)$.
Also hat das Minimalpolynom von α mindestens Grad 4 und f ist bereits das Minimalpolynom.

Aufgabe 2 (Frühjahr 2014)**.** Es seien p eine Primzahl, $\mathbb{F}_p$ der Körper mit p Elementen, $\mathbb{F}_p(t)$ der Quotientenkörper des Polynomrings $\mathbb{F}_p[t]$, und $\mathbb{F}_p(t^p)$ der kleinste Teilkörper von $\mathbb{F}_p(t)$, der t^p enthält.

(a) Zeigen Sie, daß das Polynom $X^p - t^p \in \mathbb{F}_p(t^p)[X]$ irreduzibel ist.

(b) Zeigen Sie, daß die Körpererweiterung $\mathbb{F}_p(t) \supset \mathbb{F}_p(t^p)$ endlich und normal aber nicht separabel ist.

Lösung. **Zu (a):** Über dem Körper $\mathbb{F}_p(t)$ zerfällt das Polynom

$$f := x^p - t^p = (x-t)^p$$

in identische Linearfaktoren. Wir zeigen, daß jede Zerlegung von f über $\mathbb{F}_p(t^p)$ trivial ist. Sei also $f = gh$, mit $g, h \in \mathbb{F}_p(t^p)[X]$. Ohne Einschränkung (nach Multiplikation mit dem Leitkoeffizienten von g beziehungsweise h) seien g und h normiert. Da f über $\mathbb{F}_p(t)$ in p Linearfaktoren der Form $X - t$ zerfällt, müßen auch g und h Potenzen des Linearfaktors $X - t$ sein. Also gibt es eine natürliche Zahl m, $0 \leqslant m \leqslant p$ mit $g = (X-t)^m$ und $h = (X-t)^{p-m}$.
Dann ist $d = (-1)^m t^m \in \mathbb{F}_p(t^p)$ der konstante Term von g. Nach Definition gilt

$$\mathbb{F}_p(t^p) = \left\{ \frac{u(t^p)}{v(t^p)} \;\middle|\; u, v \in \mathbb{F}_p[X] \right\}.$$

Also gibt es $u, v \in \mathbb{F}_p[X]$ mit

$$(-1)^m t^m = d = \frac{u(t^p)}{v(t^p)}.$$

Also gilt

$$(-1)^m t^m v(t^p) = u(t^p).$$

Es gilt $p | \deg(u(t^p))$ und $p | \deg(v(t^p))$, also auch $p | \deg(t^m) = m$. Dies ist nur möglich, wenn $m = 0$ oder $m = p$. Im ersten Fall ist $g = f$, im zweiten Fall ist $h = f$.

Zu (b): Es gilt $\mathbb{F}_p(t) = \mathbb{F}_p(t^p)(t)$ und t ist eine Nullstelle des Polynoms f. Da f über $\mathbb{F}_p(t^p)$ irreduzibel ist, ist es das Minimalpolynom von t über $\mathbb{F}_p(t^p)$. Also ist die Erweiterung $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ endlich und algebraisch (sogar einfach), vom Grad

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

Da f über $\mathbb{F}_p(t)$ in Linearfaktoren zerfällt und von der einzigen Nullstelle t von f erzeugt wird, ist $\mathbb{F}_p(t)$ Zerfällungskörper von f über $\mathbb{F}_p(t^p)$, also $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ normal.
Es ist klar, daß f nicht separable ist, da es in dem Zerfällungskörper $\mathbb{F}_p(t)$ die p-fache Nullstelle t besitzt. (Außerdem ist $f' = pX^{p-1} = 0$.) Somit ist das Element $t \in \mathbb{F}_p(t)$ nicht separabel über $\mathbb{F}_p(t^p)$, also $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ nicht separabel.

Aufgabe 3 (Frühjahr 2000)**.** (a) Man bestimme ein primitives Element für die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})/\mathbb{Q}$.

(b) Seien x und y Unbestimmte über dem Körper $\mathbb{F}_p$ von p Elementen. Man zeige: Die Körpererweiterung $\mathbb{F}_p(x,y)/\mathbb{F}_p(x^p, y^p)$ besitzt kein primitives Element.

Lösung. **Zu (a):** Es ist klar, daß die Erweiterung $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})/\mathbb{Q}$ separabel ist, denn $\mathbb{Q}$ und somit $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$ haben Charakteristik 0. Genauer: Die Minimalpolynome von $\sqrt[3]{2}$ und $\sqrt[4]{5}$ über $\mathbb{Q}$ sind nach Definition irreduzibel, und alle irreduziblen Polynome über einem Körper der Charakteristik 0 sind separabel. Also sind die Elemente $\sqrt[3]{2}$ und $\sqrt[4]{5}$ separabel, und damit ist die Erweiterung $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})/\mathbb{Q}$ separabel.
Nach dem Satz vom primitiven Element gibt es also α mit $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$. Wir "raten" ein solches Element.
Da einerseits 2 und 5 verschiedene Primzahlen sind, und andererseits 3 und 4 relativ prim, ist $\alpha = \sqrt[3]{2} \cdot \sqrt[4]{5}$ ein guter Kandidat.
Es ist klar, daß $\alpha \in \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$, also $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$.
Nach dem chinesischen Restsatz gibt es $a, b \in \mathbb{Z}$ (sogar $\in \mathbb{N}$) mit

$$\begin{array}{llll} a \equiv 0 \mod 4 & b & \equiv 1 \mod 4 \\ a \equiv 1 \mod 3 & b & \equiv 0 \mod 3 \end{array}$$

Man sieht leicht, daß dies zum Beispiel für $a = 4$ und $b = 9$ gilt. Also ist $\alpha^4 = \sqrt[3]{2}^4 \cdot 5 = 2 \cdot 5 \cdot \sqrt[3]{2}$, also

$$\sqrt[3]{2} = \frac{\alpha^4}{10}.$$

Weiter ist $\alpha^9 = 2^3 \sqrt[4]{5}^9 = 2^3 \cdot 5^2 \cdot \sqrt[4]{5}$ also

$$\sqrt[4]{5} = \frac{\alpha^9}{2^3 \cdot 5^2}.$$

Damit ist $\sqrt[3]{2}, \sqrt[4]{5} \in \mathbb{Q}(\alpha)$, also $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5}) \subset \mathbb{Q}(\alpha)$.
Insgesamt $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5}) = \mathbb{Q}(\alpha)$, und α ist ein primitives Eement.

Zu (b): Wir bestimmen zunächst den Grad der Erweiterung $\mathbb{F}_p(x,y)/\mathbb{F}_p(x^p, y^p)$. Da x und y algebraisch unabhängig über $\mathbb{F}_p$ sind, gilt dies auch für x^p und y^p. Insbesondere sind x^p und y^p Primelemente in $\mathbb{F}_p[x^p, y^p]$. Das Polynom $X^p - x^p$ in $\mathbb{F}_p(x^p, y^p)[X]$ sind irreduzibel nach Eisenstein (oder wie schon in der vorherigen Aufgabe gezeigt), und hat x als Nullstelle. Also ist es das Minimalpolynom von x über $\mathbb{F}_p(x^p, y^p)$ und die Erweiterung $\mathbb{F}_p(x^p, y^p)(x) = \mathbb{F}_p(x, y^p)/\mathbb{F}_p(x^p, y^p)$ hat Grad p. Ebenso ist $X^p - y^p \in \mathbb{F}_p(x^p, y^p)[X] \subset \mathbb{F}_p(x, y^p)[X]$ irreduzibel, und y eine Nullstelle. Also ist $X^p - y^p$ das Minimalpolynom von y über $\mathbb{F}_p(x, y^p)$. Die Erweiterung $\mathbb{F}_p(x, y^p)(y) = \mathbb{F}_p(x,y)/\mathbb{F}_p(x, y^p)$ hat Grad p. Nach dem Gradsatz ist

$$[\mathbb{F}_p(x,y) : \mathbb{F}_p(x^p, y^p)] = [\mathbb{F}_p(x,y) : \mathbb{F}_p(x, y^p)] \cdot [\mathbb{F}_p(x, y^p) : \mathbb{F}_p(x^p, y^p)] = p^2.$$

Als nächstes machen wir folgende Beobachtung: Da $\mathbb{F}_p(x,y)$ wie $\mathbb{F}_p$ die Charakteristik p hat, ist die Abildung

$$\sigma : \mathbb{F}_p(x,y) \to \mathbb{F}_p(x,y), \alpha \mapsto \alpha^p$$

ein Körperhomomorphismus, also injektiv. Genauer gilt für jedes $\alpha \in \mathbb{F}_p(x,y)$ daß $\alpha^p \in \mathbb{F}_p(x^p, y^p)$ ist. Ist nämlich $\alpha = \frac{f(x,y)}{g(x,y)}$, so ist $\alpha^p = \frac{f(x^p, y^p)}{g(x^p, y^p)}$. Beachte, daß die Koeffizienten von g und f in $\mathbb{F}_p$ sind, wo σ die Identität ist.
Schließlich verwenden wir diese Informationen in einem Widerspruchsbeweis. Angenommen, die Erweiterung $\mathbb{F}_p(x,y)/\mathbb{F}_p(x^p, y^p)$ wäre einfach und α ein primitives Element, also $\mathbb{F}_p(x,y) = \mathbb{F}_p(x^p, y^p)(\alpha)$. Da nach $\alpha^p \in \mathbb{F}_p(x^p, y^p)$ ist das Polynom $X^p - \alpha^p \in \mathbb{F}_p(x^p, y^p)[X]$ und α ist eine Nullstelle davon. Also teilt das Minimalpolynom von α über $\mathbb{F}_p(x^p, y^p)$ dieses Polynom und hat damit Grad $\leqslant p$. Dies würde bedeuten $[\mathbb{F}_p(x^p, y^p)(\alpha) : \mathbb{F}_p(x^p, y^p)] \leqslant p$, ein Widerspruch zu $[\mathbb{F}_p(x,y) : \mathbb{F}_p(x^p, y^p)] = p^2$. Also ist die Erweiterung $\mathbb{F}_p(x,y)/\mathbb{F}_p(x^p, y^p)$ nicht einfach.

Aufgabe 4. Sei $\mathrm{char}(K) = p$ und $\alpha \in K$. Das Polynom $f = X^p - \alpha$ ist genau dann irreduzibel in $K[X]$, wenn es in K keine Nullstellen hat.

Lösung. Wir nehmen zunächst an, daß f in K eine Nullstelle x hat. Dann ist $\alpha = x^p$ und es gilt

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

Damit ist f reduzibel.
Habe andererseits f keine Nullstelle in K. Es gibt eine endliche Erweiterung $K \subset L$ und $x \in L \backslash K$ mit $f(x) = 0$. Dann ist $\alpha = x^p$ und $f = (X - x)^p$. Angenommen es gibt $g, h \in K[X]$, so daß $f = gh$. Ohne Einschränkung kann man annehmen, daß g und h normiert sind. Dann existieren $a, b \in \mathbb{N}$, mit $a + b = p$ und $g = (X - x)^a$ sowie $h = (X - x)^b$. Es folgt, dass $x^a, x^b \in K$. Wegen $1 \leqslant a < p$ sind a und p relativ prim und es gibt $u, v \in \mathbb{Z}$ mit $au + pv = 1$. Es folgt $x = x^{av} x^{pu} \in K$, was ein Widerspruch zur Annahme ist.