Lösungen zu Übungsblatt 7
Modul Algebra 2, SoSe 2006

(19) (a) (i) Sei $p = 5$. Dann ist $g(0) = 1, g(1) = 3, g(2) = 2, g(3) = 3, g(4) = 1$, also $g(x) \neq 0$ für alle $x \in \mathbb{Z}_5$. Somit ist g unzerlegbar über $\mathbb{Z}_5$ und damit ist nach Vorlesung $\mathbb{Z}_5[x]_{2,g}$ ein Körper. Da die Elemente in $\mathbb{Z}_5[x]_{2,g}$ alle die Gestalt $ax + b$ mit $a, b \in \mathbb{Z}_5$ haben, besitzt dieser $5^2 = 25$ Elemente.

(ii) Sei $p = 7$. Dann ist $g(2) = g(4) = 0$. Somit ist g nicht unzerlegbar und damit $\mathbb{Z}_7[x]_{2,g}$ kein Körper. (z.B. $(x - 2)$ ist Nullteiler.)

(iii) Sei $p = 11$. Hier gilt wieder $g(x) \neq 0$ für alle $x \in \mathbb{Z}_{11}$. Somit ist $\mathbb{Z}_{11}[x]_{2,g}$ Körper mit $11^2 = 121$ Elementen.

(b) Zu berechnen ist $(x^2 + 1)^{\textcircled{-1}}$ in $\mathbb{Z}_p[x]_{2,g}$ für $p \in \{5, 7, 11\}$.
Dazu berechnen wir zunächst $\varrho_g(x^2+1)$, also den Rest der Polynomdivision $(x^2 + 1) : (x^2 + x + 1)$, und erhalten $\varrho_g(x^2 + 1) = -x$. Dann berechnen wir einen $\mathsf{ggT}(x, g)$. Falls dieser $= 1$ ist, erhält man $r, s \in \mathbb{Z}_p[x]$ mit $(-x)r + gs = 1$, also ist $(-x) \odot_g \varrho_g(r) = 1$. Somit ist $\varrho_g(r)$ die multiplikative Inverse zu $-x$ in $\mathbb{Z}_p[x]_{2,g}$.
Zur Berechnung:

$$\left|\begin{array}{c|cc} -x & 1 & 0 \\ x^2+x+1 & 0 & 1 \end{array}\right| \rightsquigarrow \left|\begin{array}{c|cc} -x & 1 & 0 \\ x+1 & x & 1 \end{array}\right| \rightsquigarrow \left|\begin{array}{c|cc} 1 & x+1 & 1 \\ 0 & * & * \end{array}\right|$$

Damit ist $(-x)(x+1)+(x^2+x+1)(-1) = 1$, und zwar unabhängig von p. Somit ist $(x+1)$ die gesuchte Inverse für jedes der $p \in \{5, 7, 11\}$, und damit insbesondere auch für $p = 7$, obwohl $\mathbb{Z}_7[x]_{2,g}$ nach Teil (a) kein Körper ist.

(20) (a) Gezeigt werden soll $\ker \pi_\alpha = gK[x]$.
Zunächst zeigen wir '$\supseteq$': Sei $h \in K[x]$, dann ist $\pi_\alpha(gh) = g(\alpha)h(\alpha) = 0$, also $gh \in \ker(\pi_\alpha)$.
Jetzt die nicht ganz so triviale Rückrichtung '$\subseteq$':
Da $K[x]$ Hauptidealbereich ist, gilt für ein $\hat{g} \in K[x]$:

$$gK[x] \subseteq \ker \pi_\alpha = \hat{g}K[x].$$

Das Polynom g ist irreduzibel, also ist $gK[x]$ ein maximales Ideal in $K[x]$. Da $gK[x]$ in $\hat{g}K[x]$ enthalten ist, gilt entweder $g = \hat{g}$ oder $\hat{g}K[x] = K[x]$. Letzteres würde aber bedeuten, dass α Nullstelle jedes Polynoms aus $K[x]$ wäre, was offensichtlich falsch ist. Also ist $\ker \pi_\alpha = gK[x]$. □

(b) α ist Nullstelle von $g := x^3 - x - 1$, denn es ist $\alpha^3 = \alpha + 1$ nach Voraussetzung. g ist irreduzibel, $K[\alpha]$ ist ein Körper, und $K[\alpha] \cong K[x]_{3,g}$, wobei der Isomorphismus α in x überführt. Zunächst berechnen wir $\varrho_g(x^5 - x^2 + x + 1) = 2 + 2x$. Entsprechend ist $\alpha^5 - \alpha^2 + \alpha + 1 = 2 + 2\alpha \neq 0$ der Nenner unseres Ausdrucks und dieser ist somit wohldefiniert. Indem wir eine Rechnung analog zu Aufgabe (18b) durchführen stellen wir fest, dass $\mathsf{ggT}(2 + 2x, g) = 1$ ist, und erhalten die Bézoutidentität

$$(2x + 2)(\frac{x^2}{2} - \frac{x}{2}) + (x^3 - x - 1)(-1) = 1.$$

Daher ist $\varrho_g(\frac{x^2}{2} - \frac{x}{2}) = \frac{x^2}{2} - \frac{x}{2}$ die Inverse von $(2 + 2x)$ in $K[x]_{3,g}$ und es gilt entsprechend

$$(2 + 2\alpha)^{-1} = \frac{\alpha^2}{2} - \frac{\alpha}{2}.$$

Da weiter

$$\varrho_g\big((x^5+2x^2-x+1)(\frac{x^2}{2}-\frac{x}{2})\big)=\frac{5}{2}\,x^2-x-\frac{3}{2}\,,$$

gilt entsprechend

$$(\alpha^5+2\alpha^2-\alpha+1)(\frac{\alpha^2}{2}-\frac{\alpha}{2})=\frac{5}{2}\alpha^2-\alpha-\frac{3}{2}\,,$$

und das gesuchte Ergebnis ist:

$$a=\frac{5}{2},\quad b=-1,\quad c=-\frac{3}{2}\,.$$

(21) (a) Zunächst zeigen wir, dass ε K-linear ist.
Für $(b_0,\ldots,b_{k-1})$ und $(c_0,\ldots,c_{k-1})\in K^k$ gilt:

$\varepsilon((b_0,\ldots,b_{k-1})+(c_0,\ldots,c_{k-1}))$
$=\varepsilon(b_0+c_0,\ldots,b_{k-1}+c_{k-1})=\pi(\sum_{\mu=0}^{k-1}(b_\mu+c_\mu)x^\mu)$
$=(\sum_{\mu=0}^{k-1}(b_\mu+c_\mu)\alpha_1^\mu,\ldots,\sum_{\mu=0}^{k-1}(b_\mu+c_\mu)\alpha_n^\mu)$
$=(\sum_{\mu=0}^{k-1}b_\mu\alpha_1^\mu+\sum_{\mu=0}^{k-1}c_\mu\alpha_1^\mu,\ldots,\sum_{\mu=0}^{k-1}b_\mu\alpha_n^\mu+\sum_{\mu=0}^{k-1}c_\mu\alpha_n^\mu)$
$=(\sum_{\mu=0}^{k-1}b_\mu\alpha_1^\mu,\ldots,\sum_{\mu=0}^{k-1}b_\mu\alpha_n^\mu)+(\sum_{\mu=0}^{k-1}c_\mu\alpha_1^\mu,\ldots,\sum_{\mu=0}^{k-1}c_\mu\alpha_n^\mu)$
$=\varepsilon((b_0,\ldots,b_{k-1}))+\varepsilon((c_0,\ldots,c_{k-1}))$.

Mit $\lambda\in K$ gilt:
$\varepsilon(\lambda(b_0,\ldots,b_{k-1}))=\varepsilon((\lambda b_0,\ldots,\lambda b_{k-1}))$
$=\pi(\sum_{\mu=0}^{k-1}\lambda b_\mu x^\mu)=(\sum_{\mu=0}^{k-1}\lambda b_\mu\alpha_1^\mu,\ldots,\sum_{\mu=0}^{k-1}\lambda b_\mu\alpha_n^\mu)$
$=\lambda(\sum_{\mu=0}^{k-1}b_\mu\alpha_1^\mu,\ldots,\sum_{\mu=0}^{k-1}b_\mu\alpha_n^\mu)=\lambda\cdot\varepsilon((b_0,\ldots,b_{k-1}))$.

Also ist ε K-linear.
Jetzt zeigen wir, dass ε injektiv ist. Dazu zeigen wir, dass $\ker(\varepsilon)=\{0\}$ ist.
'$\supseteq$' ist klar. '$\subseteq$': Sei $\varepsilon((b_0,\ldots,b_{k-1}))=0$, dann ist

$$0=\pi(\sum_{\mu=0}^{k-1}b_\mu x^\mu)=(f(\alpha_1),\ldots,f(\alpha_n))\quad\text{mit}\quad f=\sum_{\mu=0}^{k-1}b_\mu x^\mu.$$

Falls $f\neq 0$, dann ist f ein Polynom mit einem Grad $\leq k-1$, das n paarweise verschiedene Nullstellen hat, wobei $k-1<n$. Nach § 9 (Abschnitt zur Interpolation) ist das Nullpolynom die einzige Lösung von Grad $<n$ des Interpolationsproblems

$$f(\alpha_1)=0,\ldots,f(\alpha_n)=0\,.$$

Es folgt $f=0$, bzw. $b_0=b_1=\cdots=b_{k-1}=0$.

(b) Wir nehmen an, $\varepsilon(u)-\varepsilon(v)$ habe k Nulleinträge, also sei ohne Einschränkung $(\varepsilon(u)-\varepsilon(v))_i=(\varepsilon(u-v))_i=0$ für $i\in\{0,\ldots,k-1\}$ nach einer entsprechenden Umnummerierung der α_i. Dann ist $\sum_{\mu=0}^{k-1}(u_\mu-v_\mu)\alpha_i^\mu=0$ für $i\in\{0,\ldots,k-1\}$. Also gilt: $\sum_{\mu=0}^{k-1}(u_\mu-v_\mu)x^\mu$ hat k Nullstellen. Mit der gleichen Begründung wie in (a) ergibt sich $(u_\mu-v_\mu)=0$ für $\mu\in\{0,\ldots,k-1\}$, was ein Widerspruch zur Annahme $u\neq v$ ist. □