N. Krauß, M. Künzer

Algebra für Lehramt, SoSe 21

Lösung 12

Aufgabe 45 Sei $n \geqslant 1$. Man bestimme das Kreisteilungspolynom $\Phi_n(X)$ in folgenden Fällen.

(1) $n = 8$

(2) $n = 12$

(3) $n = 14$

(4) $n = 30$

Lösung zu Aufgabe 45:

(1) Es ist $X^8 - 1 = \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_4(X) \cdot \Phi_8(X)$. Mit $X^4 - 1 = \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_4(X)$ folgt

$$\Phi_8(X) = \frac{X^8 - 1}{X^4 - 1} = X^4 + 1 \ .$$

(2) Es ist $X^{12} - 1 = \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_3(X) \cdot \Phi_4(X) \cdot \Phi_6(X) \cdot \Phi_{12}(X)$.

Es ist $X^6 - 1 = \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_3(X) \cdot \Phi_6(X)$ und $\Phi_4(X) = \dfrac{X^4 - 1}{\Phi_1(X) \cdot \Phi_2(X)} = \dfrac{X^4 - 1}{X^2 - 1} = X^2 + 1$.

Nun folgt

$$\Phi_{12}(X) = \frac{X^{12} - 1}{(X^6 - 1) \cdot (X^2 + 1)} = \frac{X^6 + 1}{X^2 + 1} = X^4 - X^2 + 1 \ .$$

(3) Es ist $X^{14} - 1 = \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_7(X) \cdot \Phi_{14}(X)$.

Es ist $X^7 - 1 = \Phi_1(X) \cdot \Phi_7(X)$ und $\Phi_2(X) = \dfrac{X^2 - 1}{\Phi_1(X)} = \dfrac{X^2 - 1}{X - 1} = X + 1$.

Nun folgt

$$\Phi_{14}(X) = \frac{X^{14} - 1}{(X^7 - 1) \cdot (X + 1)} = \frac{X^7 + 1}{X + 1} = X^6 - X^5 + X^4 - X^3 + X^2 - X + 1 \ .$$

(4) Es ist $X^{30} - 1 = \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_3(X) \cdot \Phi_5(X) \cdot \Phi_6(X) \cdot \Phi_{10}(X) \cdot \Phi_{15}(X) \cdot \Phi_{30}(X)$.

Es ist $X^{15} - 1 = \Phi_1(X) \cdot \Phi_3(X) \cdot \Phi_5(X) \cdot \Phi_{15}(X)$.

Es ist $X^{10} - 1 = \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_5(X) \cdot \Phi_{10}(X)$.

Es ist $X^6 - 1 = \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_3(X) \cdot \Phi_6(X)$.

Es ist $X^5 - 1 = \Phi_1(X) \cdot \Phi_5(X)$.

Nun ist

$$
\begin{aligned}
\Phi_{30}(X) &= \frac{X^{30}-1}{\Phi_1(X)\cdot\Phi_2(X)\cdot\Phi_3(X)\cdot\Phi_5(X)\cdot\Phi_6(X)\cdot\Phi_{10}(X)\cdot\Phi_{15}(X)}\cdot\frac{\Phi_1(X)\cdot\Phi_5(X)\cdot\Phi_1(X)\cdot\Phi_2(X)\cdot\Phi_3(X)}{\Phi_1(X)\cdot\Phi_5(X)\cdot\Phi_1(X)\cdot\Phi_2(X)\cdot\Phi_3(X)}\\
&= \frac{X^{30}-1}{(X^{15}-1)\cdot(X^{10}-1)\cdot(X^6-1)}\cdot\Phi_1(X)\cdot\Phi_5(X)\cdot\Phi_1(X)\cdot\Phi_2(X)\cdot\Phi_3(X)\\
&= \frac{X^{30}-1}{(X^{15}-1)\cdot(X^{10}-1)\cdot(X^6-1)}\cdot(X^5-1)\cdot(X+1)\cdot(X^3-1)\\
&= \frac{(X^{15}+1)\cdot(X^5-1)\cdot(X+1)\cdot(X^3-1)}{(X^{10}-1)\cdot(X^6-1)}\\
&= \frac{(X^{15}+1)\cdot(X^5-1)\cdot(X+1)\cdot(X^3-1)}{(X^5+1)\cdot(X^5-1)\cdot(X^3-1)\cdot(X^3+1)}\\
&= \frac{(X^{15}+1)\cdot(X+1)}{(X^5+1)\cdot(X^3+1)}\\
&= \frac{X^{10}-X^5+1}{X^2-X+1}\\
&\overset{\text{Polynomdivision}}{=} X^8+X^7-X^5-X^4-X^3+X+1\,.
\end{aligned}
$$

Aufgabe 46 Man bestimme folgendes.

(1) $\varphi(540)$

(2) $\mu_{\zeta_{15},\mathbb{Q}(\zeta_5)}(X)$ und eine $\mathbb{Q}(\zeta_5)$-lineare Basis von $\mathbb{Q}(\zeta_{15})$

(3) $[\mathbb{Q}(\zeta_{36}):\mathbb{Q}]$

(4) $a, b \in \mathbb{Z}_{\geqslant 1}$ mit $a \neq b$ und $\varphi(a) = \varphi(b) = 24$.

Lösung zu Aufgabe 46:

(1) Es ist

$$\varphi(540) = \varphi(2^2\cdot 3^3\cdot 5^1) = \varphi(2^2)\cdot\varphi(3^3)\cdot\varphi(5^1) = (2-1)\cdot 2^{2-1}\cdot(3-1)\cdot 3^{3-1}\cdot(5-1)\cdot 5^{1-1} = 144\,.$$

(2) Es ist $[\mathbb{Q}(\zeta_{15}):\mathbb{Q}] = \varphi(15) = \varphi(3)\cdot\varphi(5) = 2\cdot 4 = 8$ und $[\mathbb{Q}(\zeta_5):\mathbb{Q}] = \varphi(5) = 4$. Somit ist $\deg(\mu_{\zeta_{15},\mathbb{Q}(\zeta_5)}(X)) = [\mathbb{Q}(\zeta_{15}):\mathbb{Q}(\zeta_5)] = \frac{8}{4} = 2$.
Es ist $\zeta_{15}^3 = \zeta_5$ und also ζ_{15} Nullstelle von $X^3 - \zeta_5 \in \mathbb{Q}(\zeta_5)[X]$.
Es ist $(\zeta_5^2)^3 = \zeta_5^6 = \zeta_5$ und daher auch $\zeta_5^2 \in \mathbb{Q}(\zeta_5)$ Nullstelle von $X^3 - \zeta_5$. Somit ist

$$\frac{X^3-\zeta_5}{X-\zeta_5^2} = X^2 + \zeta_5^2 X + \zeta_5^4 \in \mathbb{Q}(\zeta_5)[X]$$

ein normiertes Polynom von Grad 2, welches ζ_{15} als Nullstelle hat. Also ist

$$\mu_{\zeta_{15},\mathbb{Q}(\zeta_5)}(X) = X^2 + \zeta_5^2 X + \zeta_5^4\,.$$

Es ist $(1, \zeta_{15})$ eine $\mathbb{Q}(\zeta_5)$-lineare Basis von $\mathbb{Q}(\zeta_{15})$, vgl. Lemma 195.

(3) Es ist $[\mathbb{Q}(\zeta_{36}):\mathbb{Q}] = \varphi(36) = \varphi(2^2)\cdot\varphi(3^2) = 2\cdot 2\cdot 3 = 12$.

(4) Wir suchen alle $x \in \mathbb{Z}_{\geqslant 1}$ mit $\varphi(x) = 24$. In der Aufgabenstellung gefragt waren nur zwei solche Elemente.

In der Primfaktorzerlegung von x können nur Primzahlen kleiner als 29 auftauchen, da bereits $\varphi(29) = 28 > 24$ ist.

Für $y \in \{23, 19, 17, 11\}$ ist 24 kein Vielfaches von $\varphi(y) = y - 1$. Somit können $23, 19, 17, 11$ auch nicht in der Primfaktorzerlegung von x vorkommen.

Vorkommen können somit nur $2, 3, 5, 7, 13$. Es ist

$$\begin{array}{ccccccc}
24 & = & 12 \cdot 2 & = & \varphi(13) \cdot \varphi(2^2) & = & \varphi(52) \\
24 & = & 12 \cdot 2 & = & \varphi(13) \cdot \varphi(3) & = & \varphi(39) \\
24 & = & 12 \cdot 2 \cdot 1 & = & \varphi(13) \cdot \varphi(3) \cdot \varphi(2) & = & \varphi(78) \\
24 & = & 6 \cdot 4 & = & \varphi(7) \cdot \varphi(5) & = & \varphi(35) \\
24 & = & 6 \cdot 4 \cdot 1 & = & \varphi(7) \cdot \varphi(5) \cdot \varphi(2) & = & \varphi(70) \\
24 & = & 6 \cdot 2 \cdot 2 & = & \varphi(7) \cdot \varphi(3) \cdot \varphi(2^2) & = & \varphi(84) \\
24 & = & 6 \cdot 4 & = & \varphi(7) \cdot \varphi(2^3) & = & \varphi(56) \\
24 & = & 4 \cdot 6 & = & \varphi(5) \cdot \varphi(3^2) & = & \varphi(45) \\
24 & = & 4 \cdot 6 \cdot 1 & = & \varphi(5) \cdot \varphi(3^2) \cdot \varphi(2) & = & \varphi(90) \\
24 & = & 4 \cdot 6 & = & \varphi(3^2) \cdot \varphi(2^3) & = & \varphi(72)
\end{array}$$

Somit ist $\{x \in \mathbb{Z}_{\geqslant 1} : \varphi(x) = 24\} = \{35, 39, 45, 52, 56, 70, 72, 78, 84, 90\}$.

Aufgabe 47

(1) Sei $f(X) := X^3 + X^2 - X - 1 \in \mathbb{Q}[X]$. Bestimmen Sie $\mathrm{ggT}(f(X), f'(X))$. Ist $f(X)$ quadratfrei? Falls nicht, geben Sie einen nichtkonstanten quadratischen Faktor explizit an.

(2) Sei $g(X) := X^4 - 5X^2 - 4 \in \mathbb{Q}[X]$. Bestimmen Sie $\mathrm{ggT}(g(X), g'(X))$. Ist $g(X)$ quadratfrei? Falls nicht, geben Sie einen nichtkonstanten quadratischen Faktor explizit an.

(3) Sei $K = \mathbb{F}_2(T)$. Es ist $h(X) := X^2 - T \in K[X]$ irreduzibel und also quadratfrei.
Sei $L|K$ ein algebraischer Abschluss. Ist $h(X) \in L[X]$ quadratfrei?

Lösung zu Aufgabe 47:

(1) Es ist $f'(X) = 3X^2 + X^2 - X - 1$. Der Euklidsche Algorithmus liefert folgendes.

Es ist $X^3 + X^2 - X - 1 = (3X^2 + 2X - 1) \cdot (\frac{1}{3}X + \frac{1}{9}) - \frac{8}{9}X - \frac{8}{9}$.

Also ist $\mathrm{ggT}(f(X), f'(X)) = \mathrm{ggT}(f'(X), -\frac{8}{9}X - \frac{8}{9})$.

Es ist $3X^2 + 2X - 1 = -\frac{8}{9}(X + 1)\frac{9}{8}(-3X + 1) = -(X + 1)(-3X + 1)$.

Also ist $\mathrm{ggT}(f(X), f'(X)) = \mathrm{ggT}(f'(X), -\frac{8}{9}X - \frac{8}{9}) = \mathrm{ggT}(-\frac{8}{9}X - \frac{8}{9}, 0) = X + 1$.

Da $\mathrm{ggT}(f(X), f'(X)) = X + 1 \neq 1$ ist, ist $f(X)$ nicht quadratfrei.

Es ist $f(X) = (X + 1) \cdot (X^2 - 1) = (X + 1)^2(X - 1)$. Der quadratische Faktor ist somit $(X + 1)^2$.

(2) Es ist $g'(X) = 4X^3 - 10X$. Der Euklidsche Algorithmus liefert folgendes.

Es ist $X^4 - 5X^2 - 4 = (4X^3 - 10X) \cdot (\frac{1}{4}X) - \frac{5}{2}X^2 - 4$.

Also ist $\mathrm{ggT}(g(X), g'(X)) = \mathrm{ggT}(g'(X), -\frac{5}{2}X^2 - 4)$.

Es ist $4X^3 - 10X = (-\frac{5}{2}X^2 - 4)(-\frac{8}{5}X) - \frac{82}{5}X$.

Also ist $\mathrm{ggT}(g(X), g'(X)) = \mathrm{ggT}(g'(X), -\frac{5}{2}X^2 - 4) = \mathrm{ggT}(-\frac{5}{2}X^2 - 4, -\frac{82}{5}X) = 1$.

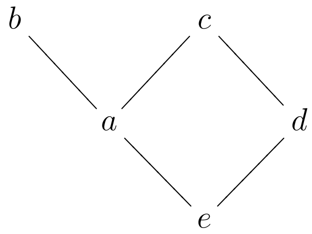
Da $\mathrm{ggT}(g(X), g'(X)) = 1$ ist, ist $g(X)$ quadratfrei.

(3) Es gibt ein Element $\omega \in L$ mit $\omega^2 = T$, da L ein algebraischer Abschluss von K ist.

Also ist $h(X) = X^2 - T = (X - \omega)(X + \omega) \overset{\mathrm{char}(L[X])=2}{=} (X - \omega)^2$ nicht quadratfrei.

Aufgabe 48 Wir betrachten das Poset

$(X, \leqslant) = (\{a, b, c, d, e\}, \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (a, c), (d, c), (e, a), (e, d), (e, c), (e, b)\})$.



(1) Bestimmen Sie alle minimalen, maximalen, initialen und terminalen Elemente in X.

(2) Man bestimme alle Ketten in X.

(3) Zeigen Sie, dass die Abbildung $f : X \to \mathrm{Pot}(X) : x \mapsto \{z \in X : z \leqslant x\}$ injektiv ist.
Gilt für $x, y \in X$ mit $x \leqslant y$, dass $f(x) \subseteq f(y)$ ist? Gibt es $x \in X$ mit $f(x) = \{a, c\}$?

Lösung zu Aufgabe 48:

(1) Es ist $e \leqslant y$ für $y \in X$, d.h. e ist initial in X. Also ist e auch minimal in X.

Für $b, c \in X$ gibt es kein $y \in X$ mit $b < y$ oder $c < y$. Somit sind b, c maximale Elemente von X. Es gibt kein terminales Element in X.

(2) Die Ketten in X sind

$$\begin{gathered}\emptyset, \\ \{a\}, \{b\}, \{c\}, \{d\}, \{e\}, \\ \{a, b\}, \{a, c\}, \{a, e\}, \{b, e\}, \{c, d\}, \{c, e\}, \{d, e\}, \\ \{a, b, e\}, \{a, c, e\}, \{c, d, e\} \ .\end{gathered}$$

(3) Seien $x, y \in X$ mit $f(x) = f(y)$.

Es ist $y \in f(x)$ und also $y \leqslant x$. Es ist $x \in f(y)$ und also $x \leqslant y$.

Somit ist $x = y$. Folglich ist f injektiv.

Alternativ: Es ist x ist terminal in $f(x)$ und y terminal in $f(y)$. Ist $f(x) = f(y)$, so folgt $x = y$, da terminale Elemente eindeutig sind, vgl. Definition 248.

Seien $x, y \in X$ mit $x \leqslant y$. Es ist $f(x) = \{z \in X : z \leqslant x\}$.

Sei $\tilde{z} \in f(x)$, dann ist $\tilde{z} \leqslant x \leqslant y$ und, da $(\leqslant)$ transitiv ist, auch $\tilde{z} \leqslant y$.

Nun folgt $\tilde{z} \in f(y) = \{z \in X : z \leqslant y\}$. Somit ist $f(x) \subseteq f(y)$.

Annahme: Es gibt $x \in X$ mit $f(X) = \{a, c\}$. Es ist c terminal in $\{a, c\}$. Also folgt $x = c$. Aber, $f(c) = \{a, c, d, e\}$. *Widerspruch.*