WS 05/06
Priv.-Doz. Dr. S. Wewers
Andreas Martin

Algebra I

10. Übungsblatt

Lösungen.

Aufgabe 1:

(a) Das Polynom $f_n := X^n + 2 \in \mathbb{Q}[X]$ ist irreduzibel nach Eisenstein.

(b) Es sei α_n eine Nullstelle von f_n in $\mathbb{C}$. Dann ist α_n algebraisch über $\mathbb{Q}$ mit

$$f_n \;=\; \mathrm{minpol}_{\mathbb{Q}}(\alpha_n)\ .$$

Es folgt $[\mathbb{Q}[\alpha_n] : \mathbb{Q}] = \deg f_n = n$. Wegen $\mathbb{Q}[\alpha_n] \subseteq \overline{\mathbb{Q}}$ folgt daher $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq n$. Da n beliebig ist, folgt daraus $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. Definitionsgemäß ist $\overline{Q}$ algebraisch über $\mathbb{Q}$.

(c) Es sei $f \in \mathbb{R}[X]$ irreduzibel und o.B.d.A. normiert. Es sei $\alpha \in \mathbb{C}$ eine Nullstelle von f. Dann ist $f = \mathrm{minpol}_{\mathbb{Q}}(\alpha)$. Wegen $[\mathbb{C} : \mathbb{R}] = 2$ folgt

$$\deg f \;=\; [\mathbb{R}[\alpha] : \mathbb{R}] \;\in\; \{1, 2\}\ .$$

(d) Es sei $f \in \mathbb{R}[X]$ von ungeradem Grade. Die Primfaktorzerlegungn von f in $\mathbb{R}[X]$ laute

$$f \;=\; p_1 \cdot \ldots \cdot p_r$$

mit irreduziblen Polynomen $p_1, \ldots, p_r \in \mathbb{R}[X]$. Nach (c) gilt $\deg p_\varrho \in \{1, 2\}$. Nach eventueller Umnumerierung können wir annehmen, daß es ein $s \in \{1, \ldots, r\}$ gibt mit $\deg p_\varrho = 1$ für $\varrho = 1, \ldots, s$ und $\deg p_\varrho = 2$ für $\varrho = s + 1, \ldots, r$. Dann gilt

$$\deg f \;=\; s + 2(r - s) \;=\; 2r - s\ .$$

Da $\deg f$ ungerade ist, muß $s \geq 1$ gelten, d.h. f besitzt einen Primfaktor in $\mathbb{R}[X]$ vom Grade 1. Dann hat f eine reelle Nullstelle.

Aufgabe 2: Als Vorbemerkung beachte man, daß in jedem kommutativen Ring R mit Einselement gilt, daß

$$a^n - 1 \;=\; (a - 1) \sum_{\nu=0}^{n-1} a^\nu$$

für alle $a \in R$ und alle $n \geq 0$. Diese Identität wird auch als *geometrische Summe* bezeichnet.

(b) Es gilt stets $X^n - 1 = \prod_{d|n} \Phi_d$. Setzt man $n := p^k$, so erhält man

$$X^{p^k} - 1 \;=\; \prod_{d|p^k} \Phi_d \;=\; \left(\prod_{d|p^{k-1}} \Phi_d \right) \Phi_{p^k} \;=\; \left(X^{p^{k-1}} - 1 \right) \Phi_{p^k}\ .$$

Ferner gilt nach obiger Vorbemerkung mit $a := X^{p^{k-1}}$

$$X^{p^k} - 1 \; = \; a^p - 1 \; = \; (a-1)\sum_{\nu=0}^{p-1} a^\nu \; = \; \left(X^{p^{k-1}} - 1\right)\sum_{\nu=0}^{p-1} X^{\nu p^{k-1}} \; .$$

Durch Gleichsetzen und Kürzen des Faktors $X^{p^{k-1}} - 1$ (der kein Nullteiler ist!) erhält man

$$\Phi_{p^k} \; = \; \sum_{\nu=0}^{p-1} X^{\nu p^{k-1}} \; .$$

Speziell gilt also

$$\Phi_p \; = \; \sum_{\nu=0}^{p-1} X^\nu \; = \; X^{p-1} + X^{p-2} + \ldots + 1 \; .$$

Zusatz: Es gilt

$$\Phi_{p^k} \; = \; \Phi_p\left(X^{p^{k-1}}\right) \; .$$

(a) Nach (b) folgt sofort

$$\begin{array}{lcccl}
\Phi_2 & & & = & X+1 \\
\Phi_3 & & & = & X^2+X+1 \\
\Phi_4 & = & \Phi_2(X^2) & = & X^2+1 \\
\Phi_5 & & & = & X^4+X^3+\ldots+1 \\
\Phi_7 & & & = & X^6+X^5+\ldots+1 \\
\Phi_8 & = & \Phi_2(X^4) & = & X^4+1 \\
\Phi_9 & = & \Phi_3(X^3) & = & X^6+X^3+1 \; .
\end{array}$$

Ferner gilt

$$\begin{array}{lcllcl}
\Phi_1 & & & & = & X-1 \\
\Phi_6 & = & \dfrac{X^6-1}{\Phi_1\cdot\Phi_2\cdot\Phi_3} & = \dfrac{(X^6-1):(X^2-1)}{X^2+X+1} & & \\
 & = & \dfrac{X^4+X^2+1}{X^2+X+1} & & = & X^2-X+1 \\
\Phi_{10} & = & \dfrac{X^{10}-1}{\Phi_1\cdot\Phi_2\cdot\Phi_5} & = \dfrac{(X^{10}-1):(X^2-1)}{X^4+X^3+\ldots+1} & & \\
 & = & \dfrac{X^8+X^6+X^4+X^2+1}{X^4+X^3+X^2+X+1} & & = & X^4-X^3+X^2-X+1 \; .
\end{array}$$

Bemerkung: Für ungerades n gilt stets $\Phi_{2n} = \Phi_n(-X)$; das folgt recht leicht durch Induktion nach n.

(c) Wir setzen $n \geq 3$ voraus. Es gilt $\zeta_n^2 - \alpha_n\zeta_n + 1 = 0$, d.h. ζ_n ist Nullstelle des Polynoms

$$f \; := \; X^2 - \alpha_n X + 1 \in \mathbb{Q}[\alpha_n][X] \; .$$

Daraus folgt, daß $\mathrm{minpol}_{\mathbb{Q}[\alpha_n]}(\zeta_n)$ ein Teiler von f ist. Es gilt trivialerweise $\mathbb{Q}[\alpha_n][\zeta_n] = \mathbb{Q}[\zeta_n]$. Somit folgt

$$[\mathbb{Q}[\zeta_n] : \mathbb{Q}[\alpha_n]] \; \in \; \{1,2\} \; .$$

Es gilt jedoch $\alpha_n = 2\,\mathrm{Re}\,\zeta_n \in \mathbb{R}$, also $\mathbb{Q}[\alpha_n] \subseteq \mathbb{R}$, währenddessen $\zeta_n \neq \mathbb{R}$ ist. Also kann der Grad $[\mathbb{Q}[\zeta_n] : \mathbb{Q}[\alpha_n]]$ nicht 1 sein. Es folgt

$$[\mathbb{Q}[\zeta_n] : \mathbb{Q}[\alpha_n]] \; = \; 2\,,$$

und

$$\mathrm{minpol}_{\mathbb{Q}[\alpha_n]}(\zeta_n) \; = \; X^2 - X + 1\,.$$

(d) Aus der Defintion von Φ_n folgt sofort, daß

$$\Phi_n(\zeta_n) \; = \; 0 \; = \; \Phi_n(\zeta_n^a)$$

für $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Da Φ_n irreduzibel und normiert ist, haben also ζ_n und ζ_n^a beide das Minimalpolynom Φ_n über $\mathbb{Q}$. Nach Vorlesung (Satz III.1.2) gibt es daher einen Isomorphismus

$$\sigma_a : K_n = \mathbb{Q}[\zeta_n] \to \mathbb{Q}[\zeta_n^a]$$

mit $\sigma_a(\zeta_n) = \zeta_n^a$. Nun gilt

$$\langle \zeta_n \rangle \; = \; \langle \zeta_n^a \rangle$$

als Untergruppe von $\mathbb{C}^\times$, denn $\mathrm{ord}(\zeta) = n$ und ggT(a,n)=1. Daher ist

$$\mathbb{Q}[\zeta_n^a] \; = \; \mathbb{Q}[\zeta_n] \; = \; K_n\,.$$

Mithin ist σ_a ein Automorphismus von K_n.

Es bleibt die Eindeutigkeit zu beweisen. Es sei dazu ϱ ein weiterer Automorphismus von K_n mit $\varrho(\zeta_n) = \zeta_n^a$. Dann ist auch $\tau := \sigma_a^{-1} \circ \varrho$ ein Automorphismus von K_n, und es gilt $\tau(\zeta_n) = \zeta_n$. Man kann nun nachrechnen (oder glauben), daß der sogenannte *Fixkörper* des Automorphismus τ

$$K_n^\tau \; := \; \{a \in K_n |\; \tau(a) = a\}$$

ein Körper ist. Nun enthält K_n^τ die Elemente $0, 1$ und ζ_n. Daher gilt $K_n^\tau = \mathbb{Q}[\zeta_n] = K_n$, d.h. τ ist die identische Abbildung. Daraus folgt $\varrho = \sigma_a$, d.h. σ_a ist eindeutig bestimmt.

Die Voraussetzung der Irreduzibilität von Φ_n war notwending, um zu schließen, daß ζ_n und ζ_n^a dasselbe Minimalpolynom haben.

Aufgabe 3:

(a) Es gilt

$$0 \; = \; \Phi_9(\zeta) \; = \; \zeta^6 + \zeta^3 + 1 \; = \; \zeta^{-3} + \zeta = 1\,.$$

Also gilt $\zeta^3 + \zeta^{-3} = -1$. Es folgt

$$\begin{aligned} \alpha &= \zeta + \zeta^{-1} \\ \alpha^2 &= \zeta^2 + 2 + \zeta^{-2} \\ \alpha^3 &= \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} \; = \; 3\alpha - 1\,. \end{aligned}$$

Also ist α Nullstelle des Polynoms

$$g \; := \; X^3 - 3X + 1\,.$$

(b) Die Reduktion modulo 2 von f ist $X^3 + X + 1$, und diese ist irreduzibel in $\mathbb{F}_2[X]$, da vom Grade 2 oder 3 und ohne Nullstelle in $\mathbb{F}_2$. Deshalb ist auch f irreduzibel in $\mathbb{Z}[X]$ und in $\mathbb{Q}[X]$.

(c) Nach (a) und (b) ist

$$\mathrm{minpol}_{\mathbb{Q}}(\alpha) \;=\; X^3 - 3X + 1 \,,$$

und es folgt

$$[\mathbb{Q}[\alpha] : \mathbb{Q}] \;=\; 3 \,.$$

Mit Aufgabe 2(c) gilt also

$$[\mathbb{Q}[\zeta] : \mathbb{Q}] \;=\; [\mathbb{Q}[\zeta] : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}]] \;=\; 2 \cdot 3 \;=\; 6 \,.$$

Nun ist Φ_9 ein normiertes Polynom vom Grade 6, welches $\Phi(\zeta_9) = 0$ erfüllt. Daher ist

$$\Phi_9 \;=\; \mathrm{minpol}_{\mathbb{Q}}(\zeta) \,,$$

also insbesondere irreduzibel.

(d) Offenbar gilt

$$\mathbb{Q}[\zeta] \;\supseteq\; \mathbb{Q}[\alpha, \zeta^3]$$

und damit

$$d \;:=\; [\mathbb{Q}[\alpha, \zeta^3] : \mathbb{Q}] \;\leq\; [\mathbb{Q}[\zeta] : \mathbb{Q}] \;=\; 6 \,.$$

Andererseits ist nach dem Gradsatz

$$\begin{aligned} d \;&=\; [\mathbb{Q}[\alpha, \zeta^3] : \mathbb{Q}[\zeta^3]] \cdot [\mathbb{Q}[\zeta^3] : \mathbb{Q}] \;=\; [\mathbb{Q}[\alpha, \zeta^3] : \mathbb{Q}[\zeta^3]] \cdot 2 \\ &=\; [\mathbb{Q}[\alpha, \zeta^3] : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}] \;=\; [\mathbb{Q}[\alpha, \zeta^3] : \mathbb{Q}[\alpha]] \cdot 3 \,; \end{aligned}$$

hierbei wurde $[\mathbb{Q}[\zeta^3] : \mathbb{Q}] = 2$ verwendet; das folgt, da $\zeta^3 = \zeta_3$ gilt und $\Phi_3 = X^2 + X + 1$ irreduzibel ist. Nach obigem sind also sowohl 2 als auch 3 Teiler von d, und daher ist auch 6 ein Teiler von d. Wegen $d \leq 6$ ist mithin $d = 6$. Die Behauptung folgt.