N. Krauß, M. Künzer

Algebra für Lehramt, SoSe 21

Lösung 11

Aufgabe 41

(1) Man bestimme alle $x \in \mathbb{F}_5$ mit $\mathrm{U}(\mathbb{F}_5) = \langle x \rangle$.

(2) Sei $\mathbb{F}_8 := \mathbb{F}_2[X]/(X^3 + X + 1)$. Sei $\beta := X + (X^3 + X + 1)$. Dann ist $\mathbb{F}_8 = \mathbb{F}_2(\beta)$ und $\beta^3 = \beta + 1$. Man bestimme alle $x \in \mathbb{F}_8$ mit $\mathrm{U}(\mathbb{F}_8) = \langle x \rangle$.

(3) Sei $\mathbb{F}_{16} := \mathbb{F}_2[X]/(X^4 + X + 1)$. Sei $\delta := X + (X^4 + X + 1)$. Dann ist $\mathbb{F}_{16} = \mathbb{F}_2(\delta)$ und $\delta^4 = \delta + 1$. Man bestimme ein $x \in \mathbb{F}_{16}$ mit $\mathrm{U}(\mathbb{F}_{16}) = \langle x \rangle$ so, dass x keine Nullstelle von $X^4 + X + 1$ ist.

(4) Sei $\mathbb{F}_{25} := \mathbb{F}_5[X]/(X^2 - 2)$. Sei $\gamma := X + (X^2 - 2)$. Dann ist $\mathbb{F}_{25} = \mathbb{F}_5(\gamma)$ und $\gamma^2 = 2$. Man bestimme ein $x \in \mathbb{F}_{25}$ mit $\mathrm{U}(\mathbb{F}_{25}) = \langle x \rangle$.

Lösung zu Aufgabe 41:

(1) Es ist $\mathrm{U}(\mathbb{F}_5) = \mathbb{F}_5^\times = \{1, 2, 3, 4\} \simeq \mathrm{C}_4$.

Es ist $|\langle 1 \rangle| = 1$ und $|\langle 4 \rangle| = |\{1, 4\}| = 2$.

Es ist

$$\langle 2 \rangle = \{2^0, 2^1, 2^2, 2^3, 2^4\} = \{1, 2, 4, 3\} = \mathrm{U}(\mathbb{F}_5) \text{ und } \langle 3 \rangle = \{3^0, 3^1, 3^2, 3^3, 3^4\} = \{1, 3, 4, 2\} = \mathrm{U}(\mathbb{F}_5)\,.$$

Somit ist $\{x \in \mathbb{F}_5 : \mathrm{U}(\mathbb{F}_5) = \langle x \rangle\} = \{2, 3\}$.

(2) Es ist $\mathrm{U}(\mathbb{F}_8) \simeq \mathrm{C}_7$ zyklisch von Ordnung 7.

Folglich ist jedes Element in $\mathrm{U}(\mathbb{F}_8) \setminus \{1\}$ von Ordnung 7, d.h.

$$\{x \in \mathbb{F}_8 : \mathrm{U}(\mathbb{F}_8) = \langle x \rangle\} = \{\beta, \beta + 1, \beta^2, \beta^2 + 1, \beta^2 + \beta, \beta^2 + \beta + 1\}\,.$$

(3) Es ist $\mathrm{U}(\mathbb{F}_{16}) \simeq \mathrm{C}_{15}$. Es ist $|\langle \delta \rangle| \in \{1, 3, 5, 15\}$ ein Teiler von 15. Wegen $\delta^1 = \delta$, $\delta^3 = \delta^3$, $\delta^5 = \delta^2 + \delta$ folgt $|\langle \delta \rangle| = 15$.

Es haben auch diejenigen Elemente δ^k Ordnung 15 für welche k teilerfremd zu 3 und 5 ist, d.h. δ^2, $\delta^4 = \delta + 1$, $\delta^7 = \delta^3 + \delta + 1$, $\delta^8 = \delta^2 + 1$, $\delta^{11} = \delta^3 + \delta^2 + \delta$, $\delta^{13} = \delta^3 + \delta^2 + 1$, $\delta^{14} = \delta^3 + 1$.

Es hat $X^4 + X + 1$ die Nullstellen $\delta, \delta^2, \delta^4 = \delta + 1, \delta^8 = \delta^2 + 1$ (Mit dem Frobeniusendomorphismus ist z.B. $0 = (\delta^4 + \delta + 1)^2 = (\delta^4)^2 + \delta^2 + 1^2 = (\delta^2)^4 + \delta^2 + 1$, usw.)

Somit ist z.B. $x := \delta^7 = \delta^3 + \delta + 1$ ein Element mit $\mathrm{U}(\mathbb{F}_{16}) = \langle x \rangle$ so, dass x keine Nullstelle von $X^4 + X + 1$ ist.

(4) Jedes Element in $\mathrm{U}(\mathbb{F}_{25}) \simeq \mathrm{C}_{24}$ hat Ordnung $1, 2, 3, 4, 6, 8, 12$ oder 24.

Beim Ausprobieren stellt man fest: Es ist $U_1 := \langle \gamma \rangle = \{1, \gamma, 2, 2\gamma, 4, 4\gamma, 3, 3\gamma\} \leqslant \mathbb{F}_{25}^\times$ eine zyklische Untergruppe von Ordnung 8.

D.h. jedes Element von U_1 hat höchstens Ordnung 8.

Es ist $U_2 = \langle \gamma+1 \rangle = \{1, \gamma+1, 2\gamma+3, 2, 2\gamma+2, 4\gamma+1, 4, 4\gamma+4, 3\gamma+2, 3, 3\gamma+3, \gamma+4\} \leqslant \mathbb{F}_{25}^\times$ eine zyklische Untergruppe von Ordnung 12.

D.h. jedes Element von U_2 hat höchstens Ordnung 12.

Es ist
$$(\gamma+2)^8 = (4\gamma+1)^4 = (-2\gamma+3)^2 = -2\gamma+2 \neq 1$$
und
$$(\gamma+2)^{12} = (4\gamma+1)^6 = (-2\gamma+3)^3 = 4 \neq 1 \ .$$
Folglich hat $\gamma + 2$ Ordnung 24 und es ist $\mathrm{U}(\mathbb{F}_{25}) = \langle \gamma + 2 \rangle$.

Konkrete Rechnung liefert $\langle \gamma{+}2 \rangle = \{(\gamma{+}2)^k : k \in [0, 23]\} = \{1, \gamma{+}2, 4\gamma{+}1, 4\gamma, 3\gamma+3, 4\gamma+2, 2, 2\gamma+4, 3\gamma{+}2, 3\gamma, \gamma{+}1, 3\gamma{+}4, 4, 4\gamma{+}3, \gamma 4, \gamma, 2\gamma{+}2, \gamma{+}3, 3, 3\gamma{+}1, 2\gamma{+}3, 2\gamma, 4\gamma{+}4, 2\gamma{+}1\} = \mathbb{F}_{25}^\times$.

Aufgabe 42 Man zeige, dass folgende Polynome irreduzibel sind.

(1) $X^7 + 26X^5 + 65X^4 - 91X + 156 \in \mathbb{Q}[X]$

(2) $(X+1)^5 + 2 \in \mathbb{Q}[X]$

Ist es möglich, das Kriterium von Eisenstein ohne vorherige Translation anzuwenden?

(3) $X^5 - 5X^3 + 1 \in \mathbb{Q}[X]$

(4) $X^2 + \sqrt[3]{5}X + 5\sqrt[3]{5} \in \mathbb{Q}(\sqrt[3]{5})[X]$

Lösung zu Aufgabe 42:

(1) Dies folgt mit Eisenstein für $p = 13$.

In der Tat sind $26 \equiv_{13} 0$, $65 \equiv_{13} 0$, $-91 \equiv_{13} 0$, $156 \equiv_{13} 0$.

Alle weiteren Koeffizienten, ausgenommen der Leitkoeffizient, sind null.

Dagegen ist $156 \not\equiv_{13^2} 0$.

Somit sind die Bedingungen von Lemma 213 erfüllt, und wir können folgern, dass das Polynom $X^7 + 26X^5 + 65X^4 - 91X + 156 \in \mathbb{Q}[X]$ irreduzibel ist.

(2) Nach Bemerkung 215 is das Polynom $m(X) := (X{+}1)^5{+}2 \in \mathbb{Q}[X]$ genau dann irreduzibel, wenn es das Polynom $\tilde{m}(X) := m(X-1) = X^5 - 2$ ist.

Mit Eisenstein für $p = 2$ folgt die Irreduzibilität von $\tilde{m}(X)$:

Es $-2 \equiv_2 0$. Alle weiteren Koeffizienten, ausgenommen der Leitkoeffizient, sind null.

Es ist $-2 \not\equiv_{2^2} 0$. Somit sind die Bedingungen von Lemma 213 erfüllt.

Es ist nicht möglich, das Kriterium von Eisenstein ohne vorherige Translation anzuwenden:

Wir erhalten

$$(X+1)^5+2 = (X^5+5X^4+10X^3+10X^2+5X+1)+2 = X^5+5X^4+10X^3+10X^2+5X+3\ .$$

Es sind 3 und 5 teilerfremd, daher ist das Kriterium von Eisenstein nicht anwendbar.

(3) Wir reduzieren modulo 2 und betrachten das Polynom $\bar{m}(X) = X^5+X^3+1 \in \mathbb{F}_2[X]$. Falls $\bar{m}(X)$ irreduzibel in $\mathbb{F}_2[X]$ ist, folgt mit Bemerkung 212 die Irreduzibilität von $m(X) = X^5 - 5X^3 + 1$ in $\mathbb{Q}[X]$.

Es hat $\bar{m}(X)$ keine Nullstelle in $\mathbb{F}_2$, kann also nicht in einen Faktor von Grad 1 und einen Faktor von Grad 4 zerfallen.

Wir müssen noch überprüfen, ob es in einen irreduziblen Faktor von Grad 2 und einen Faktor von Grad 3 zerfällt.

Es gibt in $\mathbb{F}_2[X]$ nur die Polynome X^2, X^2+1, X^2+X+1 von Grad 2.

Es ist X^2+X+1 das einzige irreduzible Polynom von Grad 2 in $\mathbb{F}_2[X]$.

Somit genügt es zu überprüfen, ob $\bar{m}(X)$ von X^2+X+1 in $\mathbb{F}_2[X]$ geteilt wird. Polynomdivision gibt

$$\bar{m}(X) = X^5+X^3+1 = (X^2+X+1)(X^3+X^2+X)+(X+1)\ .$$

Also ist $\bar{m}(X)$ nicht durch X^2+X+1 teilbar.

Somit ist $\bar{m}(X) \in \mathbb{F}_2[X]$ irreduzibel. Also ist auch $X^5 - 5X^3 + 1 \in \mathbb{Q}[X]$ irreduzibel.

(4) Es ist $\mathbb{Q}(\sqrt[3]{5}) \subseteq \mathbb{R}$.

Es hat das Polynom $X^2 + \sqrt[3]{5}X + 5\sqrt[3]{5} \in \mathbb{C}[X]$ die Nullstellen

$$x_{1,2} = \frac{-\sqrt[3]{5} \pm \sqrt{(\sqrt[3]{5})^2 - 20\sqrt[3]{5}}}{2}\ .$$

Da $(\sqrt[3]{5})^2 - 20\sqrt[3]{5} = \sqrt[3]{5}(\sqrt[3]{5}-20) < 0$ ist, liegen $x_{1,2} \notin \mathbb{R}$ und daher auch nicht in $\mathbb{Q}(\sqrt[3]{5})$. Folglich ist $X^2 + \sqrt[3]{5}X + 5\sqrt[3]{5} \in \mathbb{Q}(\sqrt[3]{5})[X]$ irreduzibel.

Aufgabe 43

(1) Man zeige $\cos(3x) = 4\cos(x)^3 - 3\cos(x)$ für $x \in \mathbb{R}$.

(2) Kann man mit Zirkel und Lineal einen Winkel von $20° = \frac{\pi}{9}$ konstruieren? Falls ja, führen Sie die Konstruktion durch. Falls nein, begründen Sie dies.

(3) Man zeige $\cos(5x) = 16\cos(x)^5 - 20\cos(x)^3 + 5\cos(x)$ für $x \in \mathbb{R}$.

(4) Kann man mit Zirkel und Lineal einen Winkel von $18° = \frac{\pi}{10}$ konstruieren? Falls ja, führen Sie die Konstruktion durch. Falls nein, begründen Sie dies.

Lösung zu Aufgabe 43:

(1) Durch Vergleich der Realteile von

$$\begin{aligned}\cos(3x) + \mathrm{i}\sin(3x) = \mathrm{e}^{3\mathrm{i}x} = (\mathrm{e}^{\mathrm{i}x})^3 &= (\cos(x) + \mathrm{i}\sin(x))^3 \\ &= \cos(x)^3 + 3\mathrm{i}\cos(x)^2\sin(x) - 3\cos(x)\sin(x)^2 - \mathrm{i}\sin(x)^3\end{aligned}$$

erhält man

$$\cos(3x) = \cos(x)^3 - 3\cos(x)\sin(x)^2 = \cos(x)^3 - 3\cos(x)(1-\cos(x)^2) = 4\cos(x)^3 - 3\cos(x)\ .$$

(2) Man kann den Winkel von 20° genau dann konstruieren, wenn cos(20°) konstruierbar ist.

Mit (1) gilt für $x = 20° = \frac{\pi}{9}$ und $a := \cos(x)$, dass

$$\frac{1}{2} = \cos(\frac{\pi}{3}) = \cos(3x) = 4a^3 - 3a\ .$$

Somit ist a Nullstelle des Polynoms $m(X) = 8X^3 - 6X - 1$.

Mit dem Eisensteinkriterium für $p = 3$ ist das Polynom $m(\frac{X+1}{2}) = X^3 + 3X^2 - 3$ irreduzibel in $\mathbb{Q}[X]$.

Nach Bemerkung 215 ist auch $m(X)$ irreduzibel in $\mathbb{Q}[X]$.

Somit folgt $[\mathbb{Q}(a) : \mathbb{Q}] = \deg(m(X)) = 3$. Also ist a nach Bemerkung 217 nicht konstruierbar.

(3) Durch Vergleich der Realteile von

$$\begin{aligned}&\cos(5x) + \mathrm{i}\sin(5x) = \mathrm{e}^{5\mathrm{i}x} = (\mathrm{e}^{\mathrm{i}x})^5 = (\cos(x) + \mathrm{i}\sin(x))^5 = \\ &\cos(x)^5 + 5\mathrm{i}\cos(x)^4\sin(x) - 10\cos(x)^3\sin(x)^2 - 10\mathrm{i}\cos(x)^2\sin(x)^3 + 5\cos(x)\sin(x)^4 + \mathrm{i}\sin(x)^5\end{aligned}$$

erhält man

$$\begin{aligned}\cos(5x) &= \cos(x)^5 - 10\cos(x)^3\sin(x)^2 + 5\cos(x)\sin(x)^4 \\ &= \cos(x)^5 - 10\cos(x)^3(1-\cos(x)^2) + 5\cos(x)(1-\cos(x)^2)^2 \\ &= 11\cos(x)^5 - 10\cos(x)^3 + 5\cos(x)^5 - 10\cos(x)^3 + 5\cos(x) \\ &= 16\cos(x)^5 - 20\cos(x)^3 + 5\cos(x)\ .\end{aligned}$$

(4) Man kann den Winkel von 18° genau dann konstruieren, wenn cos(18°) konstruierbar ist.

Mit (1) gilt für $x = \frac{\pi}{10}$ und $a := \cos(x)$, dass

$$\begin{aligned}0 &= \cos(\tfrac{\pi}{2}) = \cos(5x) \\ &= 16a^5 - 20a^3 + 5a \\ &= a(16a^4 - 20a^2 + 5)\ .\end{aligned}$$

Somit ist a Nullstelle des Polynoms $m(X) = 16X^4 - 20X^2 + 5$.

Wir berechnen die Nullstellen von $m(X)$ in $\mathbb{C}$.

Substituiere $Y := X^2$. Dann ist $16X^4 - 20X^2 + 5 = 16Y^2 - 20Y + 5$, und wir erhalten die Nullstellen

$$y_{1,2} = \frac{20 \pm \sqrt{400 - 4 \cdot 16 \cdot 5}}{2 \cdot 16} = \frac{20 \pm \sqrt{80}}{32} = \frac{5 \pm \sqrt{5}}{8} \ .$$

Resubstitution liefert die Nullstellen

$x_1 := \sqrt{\frac{5+\sqrt{5}}{8}} = \frac{1}{2}\sqrt{\frac{5+\sqrt{5}}{2}}$, $x_2 := -\frac{1}{2}\sqrt{\frac{5+\sqrt{5}}{2}}$, $x_3 := \frac{1}{2}\sqrt{\frac{5-\sqrt{5}}{2}}$ und $x_4 := -\frac{1}{2}\sqrt{\frac{5-\sqrt{5}}{2}}$.

Folglich ist $\frac{1}{16}m(X)$ ein normiertes, irreduzibles Polynom in $\mathbb{Q}[X]$, welches a als Nullstelle hat.

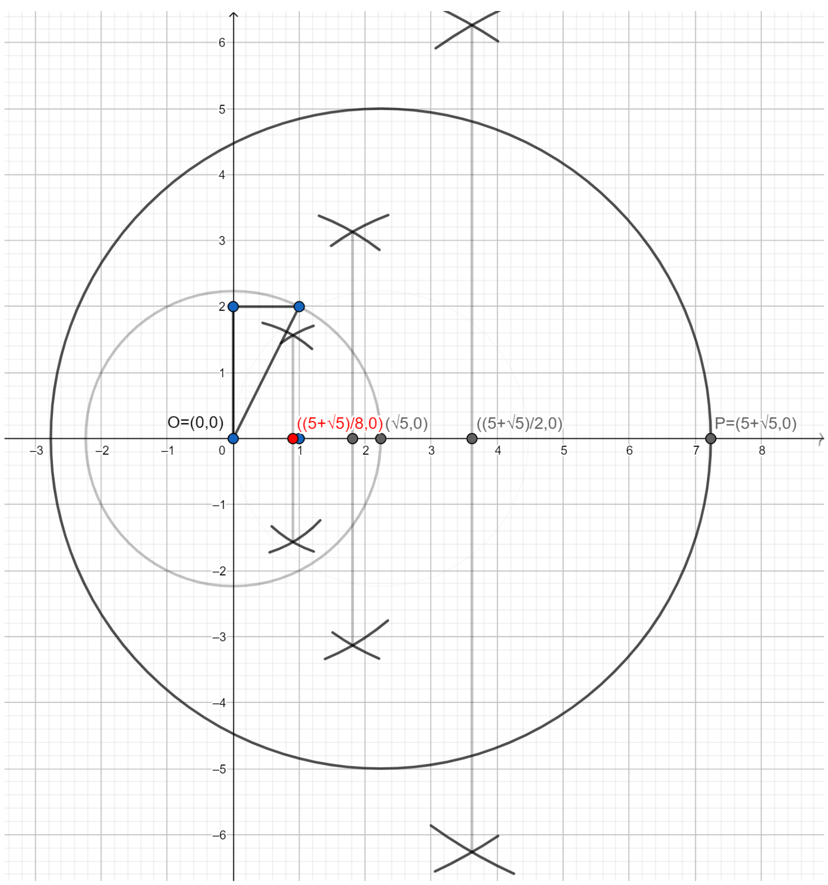
Nun ist $[\mathbb{Q}(a) : \mathbb{Q}] = \deg(m(X)) = 4 = 2^2$ und a nach Bemerkung 217 konstruierbar.

Es ist $a = \cos(\frac{\pi}{10}) > 0$, also $a \in \{x_1, x_3\}$. Nun ist $\frac{\pi}{10} < \frac{\pi}{4}$ und daher $a > \frac{1}{2}\sqrt{2} = \cos(\frac{\pi}{4})$.

Da $x_3 = \frac{1}{2}\sqrt{\frac{5-\sqrt{5}}{2}} < \frac{1}{2}\sqrt{2} < x_1 = \frac{1}{2}\sqrt{\frac{5+\sqrt{5}}{2}}$ ist, ist $a = x_1$.

Zur Konstruktion:

Wir wollen zunächst den Punkt $(\frac{5+\sqrt{5}}{8}, 0)$ konstruieren.

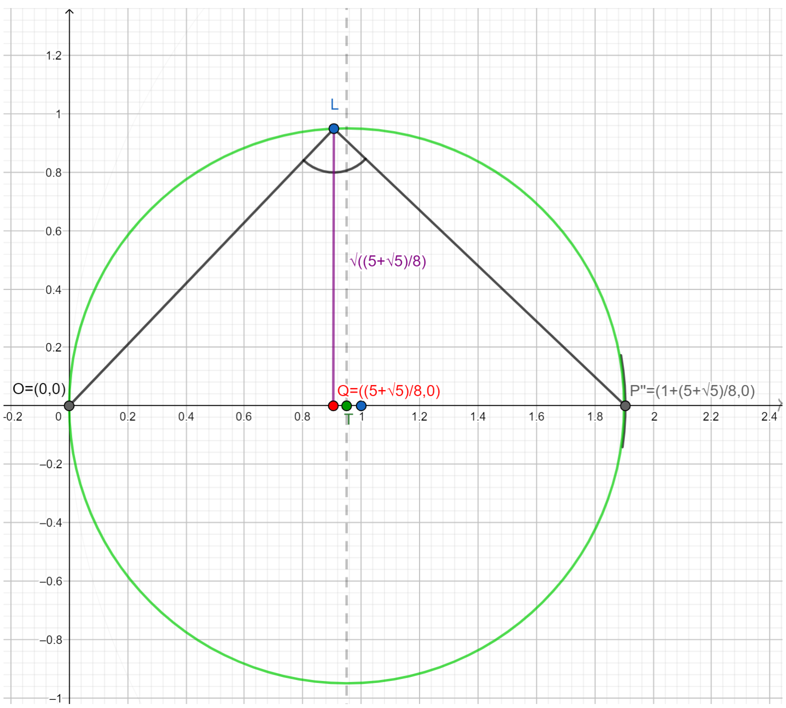


Hierfür konstruieren wir $\sqrt{5}$ als Hypotenuse eines Dreiecks mit Seitenlängen 1 und 2 und daraus den Punkt $(\sqrt{5}, 0)$.

Anschließend konstruieren wir den Punkt $P := (\sqrt{5} + 5, 0)$.

Man erhält den Punkt $P' = (\frac{5+\sqrt{5}}{2}, 0)$ durch Halbierung der Strecke OP. Erneutes Halbieren der Strecke OP' liefert $(\frac{5+\sqrt{5}}{4}, 0)$ und nochmaliges Halbieren liefert den gewünschten Punkt $(\frac{5+\sqrt{5}}{8}, 0)$.

Nun wollen wir $\sqrt{\frac{5+\sqrt{5}}{8}}$ als Höhe eines rechtwinkligen Dreiecks konstruieren.



Hierfür konstruieren wir den Punkt $P'' := (1+\frac{5+\sqrt{5}}{8}, 0)$ und den Mittelpunkt T der Strecke OP''.

Nun zeichnen wir den Thaleskreis mit Mittelpunkt T.

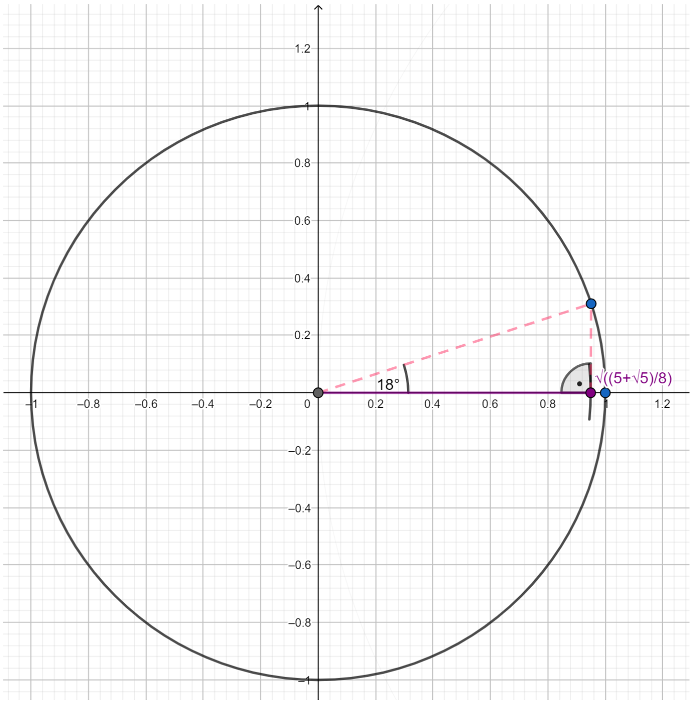
Wir errichten das Lot auf $(\frac{5+\sqrt{5}}{8}, 0)$ und erhalten den Schnittpunkt L mit dem Kreis. Dies liefert ein rechtwinkliges Dreieck $\triangle OP''L$, dessen Hypotenuse die Stecke OP'' ist.

Schreibe $a := |OL|$, $b := |LP''|$. Dann gilt für die Höhe h des Dreiecks nach dem Höhensatz

$$h^2 = \frac{5+\sqrt{5}}{8} \cdot 1$$

und daher $h = \sqrt{\frac{5+\sqrt{5}}{8}}$.

Somit konnten wir $\cos(18°)$ konstruieren und daher ergibt sich der gesuchte Winkel:



Aufgabe 44 Man zeige oder widerlege.

(1) Es hat $\mathbb{F}_{16}$ einen Teilkörper mit 8 Elementen.

(2) Sei $L|K$ eine Körpererweiterung von Grad 4 und sei $f(X) \in K[X]$ ein Polynom von Grad 3, welches eine Nullstelle in L hat. Es hat $f(X)$ eine Nullstelle in K.

(3) Sei K ein Körper und $M := \{x \in K : \text{es gibt ein } n \in \mathbb{Z}_{\geqslant 1} \text{ mit } x^n = 1.\}$. Es ist $M \leqslant \mathrm{U}(K)$.

(4) Sei K ein Körper und $M := \{x \in K : \text{es gibt ein } n \in \mathbb{Z}_{\geqslant 1} \text{ mit } x^n = 1.\}$. Es ist $|M| < \infty$.

Lösung zu Aufgabe 44:

(1) Falsch. *Angenommen* es gibt einen Teilkörper Z mit 8 Elementen. Es ist

$$\mathrm{C}_7 \simeq \mathrm{U}(Z) \leqslant \mathrm{U}(\mathbb{F}_{16}) \simeq \mathrm{C}_{15}\ .$$

Widerspruch da 7 kein Teiler ist von 15.

Alternative:

Sei Z ein Teilkörper von $\mathbb{F}_{16}$.

Es ist $\mathbb{F}_2$ enthalten in Z.

Dann ist $4 = [\mathbb{F}_{16} : \mathbb{F}_2] = [L : Z][Z : \mathbb{F}_2]$ und daher $[Z : \mathbb{F}_2] = \dim_{\mathbb{F}_2}(Z) \in \{1, 2, 4\}$ nach dem Gradsatz.

Für $[Z : \mathbb{F}_2] = 1$ folgt $Z = \mathbb{F}_2$ und also $|Z| = 2$.

Für $[Z : \mathbb{F}_2] = 4$ folgt $Z = L$ und also $|Z| = 16$.

Ist $[Z : \mathbb{F}_2] = 2$ dann gibt es eine $\mathbb{F}_2$-lineare Basis (α, β) mit $\alpha, \beta \in Z$ von Z. Also ist $|Z| = |\{a\alpha + b\beta : a, b \in \mathbb{F}_2\}| = 4$.

Somit kann es keinen Teilkörper von L mit 8 Elementen geben.

(2) Richtig. Sei $b \in L$ Nullstelle von $f(X)$.

Angenommen, $f(X)$ hat keine Nullstelle in K, dann ist $f(X)$ irreduzibel in K und, nach Division durch den Leitkoeffizienten, das Minimalpolynom von b über K.

Wir betrachten die Körpererweiterung $K(b)$ von K mit $K|K(b)|L$.

Nun ist $[K(b) : K] = 3 = \deg(f)$. Aber

$$4 = [L : K] = [L : K(b)] \cdot [K(b) : K] = [L : K(b)] \cdot 3 \ .$$

Widerspruch, da 3 nicht 4 teilt.

Also hat $f(X)$ in K eine Nullstelle.

(3) Es ist $0_K \notin M$, d.h. es ist $M \subseteq \mathrm{U}(K) = K^\times$.

Seien $x, y \in M$. Wir müssen zeigen, dass $x \cdot y^{-1} \in M$ liegt.

Es gibt $n_x, n_y \in \mathbb{Z}_{\geqslant 1}$ so, dass $x^{n_x} = 1 = y^{n_y}$.

Folglich ist $(x \cdot y^{-1})^{n_x \cdot n_y} = x^{n_x \cdot n_y} \cdot (y^{-1})^{n_x \cdot n_y} = (x^{n_x})^{n_y} \cdot (y^{n_y})^{-n_x} = 1^{n_y} \cdot 1^{-n_x} = 1$.

Es ist $n_x \cdot n_y \in \mathbb{Z}_{\geqslant 1}$ und daher $xy^{-1} \in M$. Somit ist $M \leqslant \mathrm{U}(K)$.

(4) Falsch. Sei $K = \mathbb{C}$. Jedes Element $a \in \mathbb{C}^\times$ lässt sich schreiben als $a = r \cdot \mathrm{e}^{\mathrm{i}\varphi}$ mit $r > 0$ und $0 \leqslant \varphi < 2\pi$.

Nun ist für $n \in \mathbb{Z}_{\geqslant 1}$

$$1 = a^n = r^n \, \mathrm{e}^{n\mathrm{i}\varphi} \Leftrightarrow r^n = 1 \text{ und } \mathrm{e}^{n\mathrm{i}\varphi} = 1 \Leftrightarrow r = 1 \text{ und } \varphi \in \left\{0, \frac{2\pi}{n}, \ldots, \frac{2(n-1)\pi}{n}\right\} \ ,$$

Also ist M die Menge aller Einheitswurzeln.

Der Gruppenmorphismus

$$\begin{array}{rcl} f : (\mathbb{Q}, +) & \to & (M, \cdot) \\ \frac{a}{b} & \mapsto & \mathrm{e}^{\frac{2\pi\mathrm{i}\,a}{b}} \end{array}$$

ist surjektiv. Es ist $\mathrm{Kern}(f) = \{ \frac{a}{b} \in \mathbb{Q} : \mathrm{e}^{\frac{2\pi\mathrm{i}\,a}{b}} = 1\} = \mathbb{Z}$. Nach dem Homomorphiesatz folgt $M \simeq \mathbb{Q}/\mathbb{Z}$ und daher $|M| = \infty$.

Alternativ:

Wir zeigen: Für $n, m \in \mathbb{Z}_{\geqslant 1}$ ist $\mathrm{e}^{\frac{2\pi\mathrm{i}}{n}} = \mathrm{e}^{\frac{2\pi\mathrm{i}}{m}}$ genau dann, wenn $m = n$ ist.

Sei $\mathrm{e}^{\frac{2\pi\mathrm{i}}{n}} = \mathrm{e}^{\frac{2\pi\mathrm{i}}{m}}$. Dann ist $n = |\langle \mathrm{e}^{\frac{2\pi\mathrm{i}}{n}} \rangle| = |\langle \mathrm{e}^{\frac{2\pi\mathrm{i}}{m}} \rangle| = m$.

Also existiert für jedes $n \in \mathbb{Z}_{\geqslant 1}$ ein $\mathrm{e}^{\frac{2\pi\mathrm{i}}{n}} \in M$, und diese Elemente sind paarweise verschieden. Somit ist $|M| = \infty$.