C. Dietzel, M. Künzer

Algebra für Lehramt, SoSe 20

Lösung 10

Aufgabe 37

(1) Man bestimme das Minimalpolynom $\mu_{\zeta_7+\zeta_7^{-1},\mathbb{Q}}(X) \in \mathbb{Q}[X]$.

(2) Kann man mit Zirkel und Lineal ein regelmäßiges 7-Eck konstruieren, das einem Kreis von Radius 1 einbeschrieben ist? Falls ja, führe man die Konstruktion durch. Falls nein, begründe man dies.

(3) Man bestimme das Minimalpolynom $\mu_{\zeta_5+\zeta_5^{-1},\mathbb{Q}}(X) \in \mathbb{Q}[X]$.

(4) Kann man mit Zirkel und Lineal ein regelmäßiges 5-Eck konstruieren, das einem Kreis von Radius 1 einbeschrieben ist? Falls ja, führe man die Konstruktion durch. Falls nein, begründe man dies.

Lösung zu Aufgabe 37:

(1) Nach Beispiel 224.(2) ist $\mu_{\zeta_7,\mathbb{Q}}(X) = \Phi_7(X) = X^6 + X^5 + \ldots + X + 1$. Dies bedeutet insbesondere, dass

$$\sum_{i=0}^{6} \zeta_7^i = 0$$

ist.

Wir setzen nun $\alpha = \zeta_7 + \zeta_7^{-1}$ und berechnen:

$$\begin{aligned}
\alpha &= \zeta_7 + \zeta_7^6 \\
\alpha^2 &= \zeta_7^2 + 2 + \zeta_7^{-2} \\
&= 2 + \zeta_7^2 + \zeta_7^5 \\
\alpha^3 &= \zeta_7^3 + 3\zeta_7 + 3\zeta_7^{-1} + \zeta_7^{-3} \\
&= 3\zeta_7 + \zeta_7^3 + \zeta_7^4 + 3\zeta_7^6.
\end{aligned}$$

Wir stellen nun eine nichttriviale Linearkombination von $1, \alpha, \alpha^2, \alpha^3$ her, die 0 ergibt.

$$\begin{aligned}
\alpha^3 + \alpha^2 - 2\alpha - 1 &= (3\zeta_7 + \zeta_7^3 + \zeta_7^4 + 3\zeta_7^6) + (2 + \zeta_7^2 + \zeta_7^5) \\
&\quad - 2(\zeta_7 + \zeta_7^6) - 1 \\
&= 1 + \zeta_7 + \zeta_7^2 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5 + \zeta_7^6 = 0.
\end{aligned}$$

Daraus schließen wir, dass $\mu_{\alpha,\mathbb{Q}}(X) | X^3 + X^2 - 2X - 1$ gilt. Nun hat $X^3 + X^2 - 2X - 1$ aber keine rationalen Nullstellen: nach Satz 10 sind die einzig möglichen rationalen Nullstellen 1 und -1. Durch Einsetzen überprüft man aber, dass dies keine Nullstellen sind. Nach Bemerkung 195 ist $X^3 + X^2 - 2X - 1$ also irreduzibel. Es folgt

$$\mu_{\alpha,\mathbb{Q}}(X) = X^3 + X^2 - 2X - 1.$$

(2) Sei $K \subseteq \mathbb{R}^2$ besagter Kreis und $P \in C$ gegeben. Wir dürfen ohne Einschränkung davon ausgehen, dass K den Mittelpunkt $(0,0)$ besitzt und $P = (1,0)$ ist. Könnten wir ein regelmäßiges 7-Eck mit Eckpunkten in K konstruieren, welches den Punkt P enthielte, so wären dessen Eckpunkte gerade die Punkte

$$P_k = \left(\cos\left(\frac{2\pi k}{7}\right), \sin\left(\frac{2\pi k}{7}\right)\right) \quad , \quad k \in [0,6].$$

Die von den Koordinaten von P erzeugte Erweiterung von $\mathbb{Q}$ ist natürlich $\mathbb{Q}$. Nach Bemerkung 204 sind also die Koordinaten $\cos\left(\frac{2\pi k}{7}\right), \sin\left(\frac{2\pi k}{7}\right) \in L$, wobei L ein Zwischenkörper von $\mathbb{Q}$ und $\mathbb{R}$ ist, für welchen $[L:\mathbb{Q}] = 2^n$ ist für ein $n \in \mathbb{Z}_{\geq 1}$.

Insbesondere wäre also

$$\alpha = \zeta_7 + \zeta_7^{-1} = \exp\left(\frac{2\pi \mathrm{i}}{7}\right) + \exp\left(-\frac{2\pi \mathrm{i}}{7}\right) = 2\cos\left(\frac{2\pi}{7}\right) \in L.$$

Sei $L' := \mathbb{Q}(\alpha)$. Dann ist mithilfe von Teil (1)

$$[L':\mathbb{Q}] = \deg(\mu_{\alpha,\mathbb{Q}}(X)) = 3.$$

Andererseits impliziert Lemma 193, dass $[L':\mathbb{Q}] = 3$ ein Teiler von $[L:\mathbb{Q}] = 2^n$ ist, da ja $L' \subseteq L$ und also $[L:\mathbb{Q}] = [L:L'] \cdot [L':\mathbb{Q}]$. Dies ist aber nicht der Fall. Somit ist die gefragte Konstruktion nicht durchführbar.

(3) Es ist $\mu_{\zeta_5} = \Phi_5(X) = X^4 + X^3 + \ldots + 1$, was zur Folge hat, dass

$$\sum_{i=0}^{4} \zeta_5^i = 0$$

ist.

Wir setzen $\beta = \zeta_5 + \zeta_5^{-1}$ und rechnen:

$$\begin{aligned} \beta &= \zeta_5 + \zeta_5^{-1} \\ &= \zeta_5 + \zeta_5^4 \\ \beta^2 &= \zeta_5^2 + 2 + \zeta_5^{-2} \\ &= 2 + \zeta_5^2 + \zeta_5^3 \end{aligned}$$

Weiterhin ist

$$\begin{aligned} \beta^2 + \beta - 1 &= (2 + \zeta_5^2 + \zeta_5^3) + (\zeta_5 + \zeta_5^4) - 1 \\ &= 1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0. \end{aligned}$$

Folglich gilt $\mu_{\beta,\mathbb{Q}}(X) | X^2 + X - 1$. Wie in Teil (1) stellt man fest, dass die einzig möglichen rationalen Nullstellen von $X^2 + X - 1$ die Zahlen 1 und -1 sind. Einsetzen zeigt, dass auch dies keine Nullstellen sind, folglich ist auch $X^2 + X - 1$ irreduzibel, und es folgt

$$\mu_{\beta,\mathbb{Q}}(X) = X^2 + X - 1.$$

(4) Wie in Teil (2) nehmen wir an, dass K den Mittelpunkt $(0,0)$ besitzt und $P = (1,0)$ vorgegeben ist. Wir zeigen, wie man die Punkte

$$P_k = \left(\cos\left(\frac{2\pi}{5}\right), \sin\left(\frac{2\pi}{5}\right)\right) \quad , \quad k \in [1,4]$$

konstruiert. Zusammen mit $P_0 := P$ sind dies die Eckpunkte eines regelmäßigen 5-Ecks auf K.

Zunächst wissen wir aus Teil (3), dass $\beta^2 + \beta - 1 = 0$ ist, woraus wir folgern, dass

$$\beta \in \{-\frac{1}{2} + \frac{1}{2}\sqrt{5}, -\frac{1}{2} - \frac{1}{2}\sqrt{5}\}$$

sein muss. Außerdem gilt

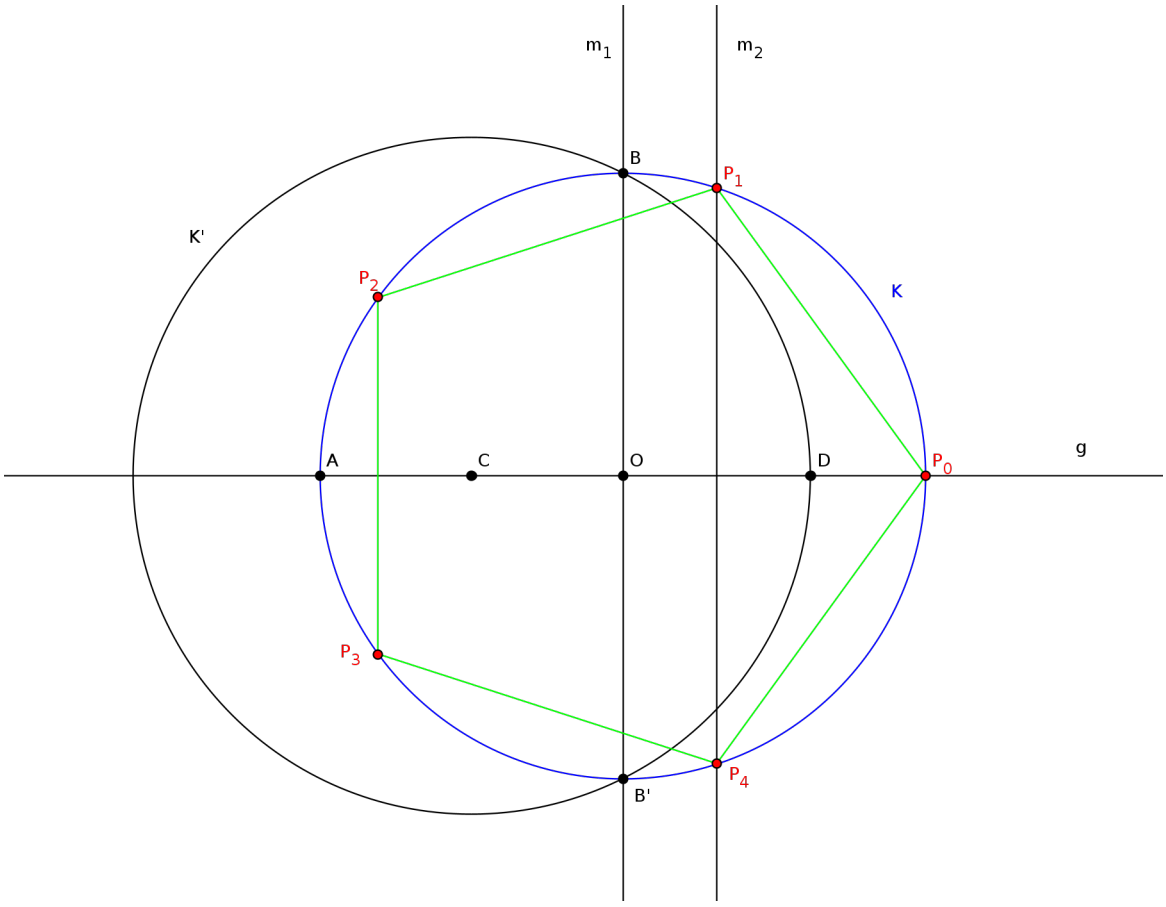
$$\beta = \zeta_5 + \zeta_5^{-1} = \exp\left(\frac{2\pi \mathrm{i} k}{5}\right) + \exp\left(-\frac{2\pi \mathrm{i} k}{5}\right) = 2\cos\left(\frac{2\pi}{5}\right) \geq 0,$$

folglich muss $\beta = -\frac{1}{2} + \frac{1}{2}\sqrt{5}$ sein. Es folgt, dass

$$\cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4}$$

sein muss. Unser Ziel ist es also, auf K den Punkt P_1 als denjenigen Punkt mit der x-Koordinate $x = \frac{-1+\sqrt{5}}{4}$ zu konstruieren, welcher im ersten Quadraten liegt.

Das folgende Bild illustriert die Konstruktion, welche wir nachfolgend im Detail erklären wollen. Hierbei gehen wir davon aus, dass bekannt ist, wie eine Mittelsenkrechte bzw. der Mittelpunkt zwischen zwei Punkten mit dem Zirkel konstruiert wird.



Sei also der Mittelpunkt $O(0/0)$, sowie der Kreis K mit dem Radius 1 um O gegeben. Außerdem sei der Punkt $P_0(1/0)$ bereits vorgegeben.

Schritt 1 Ziehe die Gerade g durch O und P_0. Diese besitzt die Gleichung

$$g : y = 0,$$

schließlich handelt es sich bei g um die x-Achse. Die Gerade g schneide den Kreis K erneut in dem Punkt A. Dieser hat die Koordinaten $A(-1/0)$.

Schritt 2 Stelle die Mittelsenkrechte m_1 zwischen A und P_0 auf. Eine Gleichung für m_1 ist gegeben durch

$$m_1 : x = 0.$$

Seien B, B' die Schnittpunkte von m_1 mit K. Diese haben die Koordinaten $B(0/1)$, $B(0/-1)$.

Schritt 3 Konstruiere den Punkt C als den Mittelpunkt zwischen A und O. Dieser hat die Koordinaten $C(-\frac{1}{2}/0)$.

Schritt 4 Konstruiere den Kreis K' mit dem Mittelpunkt C, welcher durch den Punkt B (bzw. B') geht. Sei D der Schnittpunkt von g mit K', welcher zwischen C und P_0 liegt.

Nach Pythagoras ist

$$|CB| = \sqrt{|CO|^2 + |OB|^2} = \sqrt{\left(\frac{1}{2}\right)^2 + 1^2} = \frac{1}{2}\sqrt{5},$$

damit hat K' den Radius $\frac{1}{2}\sqrt{5}$. Folglich hat D die Koordinaten $D(-\frac{1}{2} + \frac{1}{2}\sqrt{5}/0)$.

Schritt 5 Konstruiere die Gerade m_2 als Mittelsenkrechte zu den Punkten O und D. Diese wird beschrieben durch die Gleichung

$$m_2 : x = \frac{-1 + \sqrt{5}}{4} = \cos\left(\frac{2\pi}{5}\right)$$

Seien P_1 und P_4 die Schnittpunkte von m_2 mit K. Folglich hat P_1 die y-Koordinate

$$y = \sqrt{1 - \cos^2\left(\frac{2\pi}{5}\right)} = \sin\left(\frac{2\pi}{5}\right).$$

Damit erhalten wir die Koordinaten

$$P_1\left(\cos\left(\frac{2\pi}{5}\right) / \sin\left(\frac{2\pi}{5}\right)\right).$$

Ähnlich erhält man die Koordinaten

$$P_4\left(\cos\left(\frac{2\pi \cdot 4}{5}\right) / \sin\left(\frac{2\pi \cdot 4}{5}\right)\right).$$

Die Punkte P_1 und P_4 sind also tatsächlich die Eckpunkte des gesuchten 5-Ecks.

Schritt 6 Den Punkt P_2 erhält man nun, indem man einen Kreis um P_1 durch den Punkt P_0 zieht und diesen Kreis mit K schneidet. Nun kann man P_3 in gleicher Weise aus P_4 und P_0 (oder P_2 und P_1) bilden.

Eine entsprechende Konstruktion für das regelmäßige 17-Eck wurde erstmals 1825 von Johannes Erchinger demonstriert.
Eine erste Konstruktion des regelmäßigen 257-Ecks geht auf Friedrich Julius Richelot (1832) zurück.
Zuletzt gelang es 1894 dem Mathematiker Johann Gustav Hermes, die Konstruktion eines regelmäßigen 65537-Ecks durchzuführen.
Selbstverständlich sind diese Konstruktionen eher ungeeignet für eine Übungsaufgabe in einer Algebra-Vorlesung.
Nimmt man die Konstruktion des regelmäßigen 3-Ecks als gegeben hin, so lassen sich die Konstruktionen aller regelmäßigen n-Ecke, von denen bekannt (!) ist, dass sie sich mit Zirkel und Lineal konstruieren lassen, auf diese wenigen Konstruktionen - die des regelmäßigen 5-Ecks eingeschlossen - zurückführen.

Aufgabe 38

Sei $n \geqslant 1$. Man bestimme das Kreisteilungspolynom $\Phi_n(X)$.

(1) $n = 11$.

(2) $n = 9$. (Vgl. Aufgabe 34.(2).)

(3) $n = 15$.

(4) $n = 18$.

Lösung zu Aufgabe 38:

(1) Die Zahl $n = 11$ ist prim. Nach Beispiel 224.(2) ist also

$$\Phi_{11}(X) = X^{10} + X^9 + \ldots + X + 1.$$

(2) In Aufgabe 34.(2) wurde bereits gezeigt, dass $\Phi_9(X) = \mu_{\zeta_9,\mathbb{Q}}(X) = X^6 + X^3 + 1$ ist. Alternativ folgt aus $X^9 - 1 = \Phi_9(X) \cdot \Phi_3(X) \cdot \Phi_1(X) = \Phi_9(X) \cdot (X^3 - 1)$ auch

$$\Phi_9(X) = (X^9 - 1)/(X^3 - 1) = X^6 + X^3 + 1\ .$$

(3) Nach Lemma 223 und Beispiel 224.(2) ist

$$\begin{aligned} X^{15} - 1 &= \Phi_{15}(X) \cdot \Phi_5(X) \cdot \Phi_3(X) \cdot \Phi_1(X) \\ &= \Phi_{15}(X) \cdot \frac{X^5 - 1}{X - 1} \cdot \frac{X^3 - 1}{X - 1} \cdot (X - 1) \\ \Rightarrow \Phi_{15}(X) &= \frac{(X^{15} - 1)(X - 1)}{(X^5 - 1)(X^3 - 1)} \\ &= \frac{X^{10} + X^5 + 1}{X^2 + X + 1} \\ &= X^8 - X^7 + X^5 - X^4 + X^3 - X + 1. \end{aligned}$$

(4) Nach Lemma 223 ist

$$X^{18} - 1 = \Phi_{18}(X) \cdot \Phi_9(X) \cdot \Phi_6(X) \cdot \Phi_3(X) \cdot \Phi_2(X) \cdot \Phi_1(X).$$

Auch nach Lemma 223 ist

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

Setzen wir dies – zusammen mit der bereits bekannten Identität

$$\Phi_9(X) = X^6 + X^3 + 1 = \frac{X^9 - 1}{X^3 - 1} \quad -$$

in die obige Gleichung ein, so erhalten wir

$$\begin{aligned} X^{18} - 1 &= \Phi_{18}(X) \cdot \frac{X^9 - 1}{X^3 - 1} \cdot (X^6 - 1) \\ \Leftrightarrow \Phi_{18}(X) &= \frac{(X^{18} - 1)(X^3 - 1)}{(X^9 - 1)(X^6 - 1)} \\ \Rightarrow \Phi_{18}(X) &= \frac{X^9 + 1}{X^3 + 1} \\ &= X^6 - X^3 + 1. \end{aligned}$$

Alternativ: Nach Aufgabe 39.(1) und Teil (2) dieser Aufgabe haben wir

$$\Phi_{18}(X) = \Phi_9(-X) = X^6 - X^3 + 1.$$

Aufgabe 39 Man zeige.

(1) Sei $n \in \mathbb{Z}_{\geqslant 3}$ mit $n \equiv_2 1$ gegeben.
Es ist $\Phi_{2n}(X) = \Phi_n(-X)$.

(2) Sei p eine Primzahl. Sei $k \in \mathbb{Z}_{\geqslant 1}$.
Es ist $\Phi_{p^k}(X) = \Phi_p(X^{p^{k-1}})$.

Lösung zu Aufgabe 39:

(1) *Anmerkung:* Für $n = 1$ wäre die Aussage der Aufgabe falsch, denn es ist

$$\Phi_{2\cdot 1}(X) = X + 1 = -(-X - 1) = -\Phi_1(-X).$$

Wir setzen also voraus, dass $n \geqslant 3$ ist.

Da $\Phi_n(X)$ irreduzibel ist, ist auch $\Phi_n(-X)$ irreduzibel; vgl. Bem. 202.(2).

Ist n eine Potenz von 2, dann ist $\deg(\Phi_n(X)) = \varphi(n) = \frac{n}{2}$ gerade; vgl. Bem. 226.(4).

Ist n keine Potenz von 2, dann hat n einen ungeraden Primteiler p, und es wird $\deg(\Phi_n(X)) = \varphi(n)$ von $p - 1$ geteilt, ist also gerade; vgl. Bem. 226.(4).

Jedenfalls ist $\deg(\Phi_n(X))$ gerade und also $\Phi_n(-X)$ normiert.

Bleibt zu zeigen, daß ζ_{2n} eine Nullstelle von $\Phi_n(-X)$ ist, um $\Phi_{2n}(X) = \Phi_n(-X)$ zu erhalten; vgl. Bem. 184.(2).

Wir müssen also zeigen, daß $-\zeta_{2n}$ eine Nullstelle von $\Phi_n(X)$ ist.

Aber $\zeta_{2n}^n = \exp(\pi \mathrm{i}) = -1$ und also $-\zeta_{2n} = \zeta_{2n}^{1+n}$. Wir müssen also zeigen, daß ζ_{2n}^{1+n} eine Nullstelle von $\Phi_n(X)$ ist.

Sei $k \in [0, n-1]$ mit $2k = 1 + n$. Es ist $\zeta_{2n}^{1+n} = \zeta_{2n}^{2k} = \zeta_n^k$. Da wir die Nullstellen von $\Phi_n(X)$ aus Lem. 222 kennen, genügt es zu zeigen, daß k und n teilerfremd sind.

Sei $g \in \mathbb{Z}_{\geqslant 1}$ ein gemeinsamer Teiler von k und n. Dann ist g auch ein gemeinsamer Teiler von $2k = n + 1$ und n. Daraus folgt aber $g = 1$.

(2) Die Teiler von p^k sind die Zahlen p^i ($i \in [0,k]$). Mithilfe von Lemma 223 erhalten wir:

$$\begin{aligned} X^{p^k} - 1 &= \prod_{i=0}^{k} \Phi_{p^i}(X) \\ &= \Phi_{p^k}(X) \cdot \prod_{i=0}^{k-1} \Phi_{p^i}(X) \\ &= \Phi_{p^k}(X) \cdot \left(X^{p^{k-1}} - 1 \right). \end{aligned}$$

In Beispiel 224.(2) wurde bereits ausgeführt, dass

$$\Phi_p(X) = \frac{X^p - 1}{X - 1}$$

ist. Stellen wir also die Rechnung darüber nach $\Phi_{p^k}(X)$ um, so erhalten wir damit:

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

Aufgabe 40

(1) Man bestimme alle Primzahlen $p \in [2,13]$, für welche $X^2 + X + 1 \in \mathbb{F}_p[X]$ irreduzibel ist.

(2) Man bestimme alle Primzahlen p, für welche $X^2 + X + 1 \in \mathbb{F}_p[X]$ irreduzibel ist.

(3) Man bestimme alle $k \in \mathbb{Z}_{\geqslant 1}$ mit $\varphi(k) = 8$.

Lösung zu Aufgabe 40:

(1) Nach Bemerkung 195 ist die Irreduzibilität des Polynoms $f(X) := X^2 + X + 1 \in \mathbb{F}_p[X]$ äquivalent dazu, dass es kein $a \in \mathbb{F}_p$ gibt mit $f(a) = 0$.

Wir überprüfen den Fall $p = 2$ gesondert: wir haben $f(0) = f(1) = 1$, folglich hat $f(X)$ keine Nullstellen in $\mathbb{F}_2$.

Für $p > 2$ ist das Element $2 \in \mathbb{F}_p$ invertierbar. Wir können also folgende Manipulationen durchführen:

$$\begin{aligned} a^2 + a + 1 &= 0 \\ \Leftrightarrow 4a^2 + 4a + 4 &= 0 \\ \Leftrightarrow (2a+1)^2 + 3 &= 0 \\ \Leftrightarrow (2a+1)^2 &= -3. \end{aligned}$$

Diese Gleichung ist genau dann lösbar, wenn $b^2 = -3$ in $\mathbb{F}_p$ lösbar ist. Dies überprüfen wir durch Einsetzen. Hierbei kann man sich die Arbeit vereinfachen, indem man berücksichtigt, dass mit b stets auch $-b$ eine Lösung ist und es maximal zwei Lösungen gibt, da $\mathbb{F}_p$ ein Körper ist.

Folglich genügt, es, die Werte $0, 1, \ldots, \frac{p-1}{2}$ durchzutesten. Hat man zudem bereits eine Lösung b gefunden, so erhält man die andere als $-b$ (und ist fertig).

Damit erhalten wir die folgende Tabelle:

p	$b^2 = -3$ lösbar?	Lösungen
3	Ja	0
5	Nein	-
7	Ja	$2, 5$
11	Nein	-
13	Ja	$6, 7$

Man kann auch direkt die Existenz einer Nullstelle von $X^2 + X + 1$ in $\mathbb{F}_p$ experimentell überprüfen.x

(2) Wir gehen auch hier gemäß Bemerkung 195 vor, indem wir die Frage nach der Irreduzibilität in $\mathbb{F}_p[X]$ auf die Frage nach der Existenz von Nullstellen in $\mathbb{F}_p$ zurückführen.

Es gilt die Faktorisierung $X^3-1 = (X-1)(X^2+X+1)$. Wir setzen nun $f(X) = X^2+X+1$.

Aufgrund der obigen Faktorisierung ist jede Nullstelle $a \in \mathbb{F}_p$ von $f(X)$ auch eine Nullstelle von $X^3 - 1$, d.h. es gilt $a^3 = 1$.

Ist a zugleich eine Nullstelle des Polynoms $X - 1$, so ist $a = 1$, und damit ist

$$0 = 1^2 + 1 + 1 = 3,$$

was - bei den betrachteten Körpern - nur in $\mathbb{F}_3$ möglich ist.

Von nun an schränken wir uns auf diejenigen Fälle ein, in denen $p \neq 3$ ist.

Hat dann $f(X)$ eine Nullstelle $a \in \mathbb{F}_p$, so ist $a \neq 1$ und $a^3 = 1$. So ein Element existiert genau dann, wenn $3 \,|\, |\mathbb{F}_p^\times| = p - 1$ gilt. Folglich ist $X^2 + X + 1 \in \mathbb{F}_p[X]$ genau dann *nicht* irreduzibel, wenn $p = 3$ oder $p \equiv_3 1$ gilt.

Im Umkehrschluss ist $X^2 + X + 1 \in \mathbb{F}_p[X]$ also genau dann irreduzibel, wenn $p \equiv_3 2$ gilt.

Mit den uns zur Verfügung stehenden Mitteln lässt sich die Methode aus Teil (1) der Aufgabe leider nicht verwenden, um eine allgemeine Antwort für diese Frage zu erhalten. Dies wäre mithilfe des *quadratischen Reziprozitätsgesetzes* möglich, mit dem sich direkt entscheiden ließe, für welche Primzahlen p das Element $-3 \in \mathbb{F}_p$ ein Quadrat ist.
Auf der anderen Seite haben wir so unsere Kenntnisse über $\mathrm{U}(\mathbb{F}_p) = \mathbb{F}_p^\times$ einsetzen können.

(3) Sei $k \in \mathbb{Z}_{\geqslant 1}$.

Wir *behaupten*: $\mathrm{v}_2(k) \leqslant 4$, $\mathrm{v}_3(k) \leqslant 1$, $\mathrm{v}_5(k) \leqslant 1$ und $\mathrm{v}_p(k) = 0$ für $p \geqslant 7$ prim ist.

Dazu sei

$$k = \prod_{i=1}^{n} p_i^{\nu_i}$$

eine Primfaktorzerlegung von k, wobei wir annehmen, dass für alle $i \in [1, n]$ gilt, dass $p_i > 0$ und $\nu_i > 0$ ist. Hierbei haben wir kurz $\nu_i := \mathrm{v}_{p_i}(k)$ geschrieben. Tritt eine Primzahl in dieser Zerlegung nicht auf, so ist bei dieser die Bewertung gleich 0.

Nach Bemerkung 226.(3)+(4) ist

$$\begin{aligned} \varphi(k) &= \prod_{i=1}^{n} \varphi(p_i^{\nu_i}) \\ &= \prod_{i=1}^{n} (p_i - 1) p_i^{\nu_i - 1}. \end{aligned}$$

Ist $\varphi(k) = 8$, so zeigt diese Darstellung von $\varphi(k)$, dass $(p_i - 1)p_i^{\nu_i - 1} | 8$ für alle $i \in [1, n]$ gilt. Insbesondere gilt $p_i - 1 | 8$ für alle $i \in [1, n]$, weshalb alle $p_i \in \{2, 3, 5\}$ sein müssen.

Ist weiterhin $\nu_i > 1$ für ein $i \in [1, n]$, so ist $\varphi(k) = 8$ durch $p_i^{\nu_i - 1}$ teilbar. Da damit 8 auch durch p_i teilbar ist, ist dies nur dann möglich, wenn $p_i = 2$ ist. Insbesondere muss $\nu_i \in [1, 4]$ sein, sofern $p_i = 2$ als Primfaktor vorkommt. Ist $p_i \neq 2$, so muss $\nu_i = 1$ sein.

Dies zeigt die *Behauptung*.

Nach der obigen Diskussion lassen sich alle gesuchten Zahlen k darstellen als

$$k = 2^{\nu_1} \cdot 3^{\nu_2} \cdot 5^{\nu_3},$$

wobei $\nu_1 \in [0, 4]$ und $\nu_2, \nu_3 \in [0, 1]$ sind.

Testet man diese Fälle durch, so erhält man die folgenden Lösungen für die Gleichung $\varphi(k) = 8$:

$$\begin{aligned} k &= 2^4 = 16, \\ k &= 2^3 \cdot 3 = 24, \\ k &= 2^2 \cdot 5 = 20, \\ k &= 2 \cdot 3 \cdot 5 = 30, \\ k &= 3 \cdot 5 = 15. \end{aligned}$$

Wir haben die Lösungsmenge $\{\, k \in \mathbb{Z}_{\geqslant 1} \,:\, \varphi(k) = 8 \,\} = \{15, 16, 20, 24, 30\}$ erhalten.

`pnp.mathematik.uni-stuttgart.de/lexmath/kuenzer/alg20/`