

Aufgabe 13.

- (1) Nach der Mitternachtsformel hat $X^2 + bX + c$ genau dann keine reelle(n) Nullstelle(n) (ist also irreduzibel), wenn die Diskriminante $b^2 - 4c < 0$ ist. Ist $b^2 - 4c \geq 0$, so hat $X^2 + bX + c$ (mind.) eine reelle Nullstelle, ist also nicht irreduzibel. In $\mathbf{C}$ hat das Polynom $X^2 + bX + c$ die Nullstelle(n) $\frac{-b \pm \sqrt{b^2 - 4c}}{2}$, ist also nicht irreduzibel.
- (2) Man teste alle normierten Polynome von Grad 2 und 3 auf Nullstellen und erhält die irreduziblen Polynome
in $\mathbf{F}_2[X]$: $X^2 + X + 1$, $X^3 + X + 1$, $X^3 + X^2 + 1$;
in $\mathbf{F}_3[X]$: $X^2 + 1$, $X^2 + X - 1$, $X^2 - X - 1$, $X^3 - X + 1$, $X^3 - X - 1$, $X^3 + X^2 - 1$, $X^3 + X^2 + X - 1$,
 $X^3 + X^2 - X + 1$, $X^3 - X^2 + 1$, $X^3 - X^2 - X - 1$, $X^3 - X^2 + X + 1$.
- (3) Ein normiertes Polynom von Grad 4 ist irreduzibel genau dann, wenn es weder eine Nullstelle hat, noch Produkt zweier irreduzibler Polynome von Grad 2 ist.
Man testet alle (normierten) Polynome von Grad 4 auf Nullstellen. Aus den nullstellenfreien Polynomen werden alle Produkte von irreduziblen Polynome von Grad 2 aus (2) ausgeschlossen. Es bleiben die folgenden irreduziblen Polynome übrig: $X^4 + X + 1$, $X^4 + X^3 + 1$, $X^4 + X^3 + X^2 + X + 1$.
- (4) Nach (2) ist $X^3 - X^2 + 1$ irreduzibel in $\mathbf{F}_3[X]$. Also ist $\mathbf{F}_{27} = \mathbf{F}_3[X]/(X^3 - X^2 + 1)\mathbf{F}_3[X]$ ein Körper mit 27 Elementen. Mit $\gamma := \bar{X}$ gilt $\gamma^3 = \gamma^2 - 1$ und γ ist Nullstelle von $X^3 - X^2 + 1$ in $\mathbf{F}_{27}$. Weitere Nullstellen sind $\gamma^3 = \gamma^2 - 1$ und $\gamma^9 = -\gamma^2 - \gamma - 1$.

Aufgabe 14.

- (1) Wegen $f_3(X) = f_1(X) - f_2(X)u_1(X)$ ist $f_3(X) \in I_{f_1, f_2}$ und damit $I_{f_2, f_3} \subseteq I_{f_1, f_2}$. Wegen $f_1(X) = f_2(X)u_1(X) + f_3(X)$ ist $f_1(X) \in I_{f_2, f_3}$ und damit $I_{f_1, f_2} \subseteq I_{f_2, f_3}$. Also ist $I_{f_1, f_2} = I_{f_2, f_3}$.
- (2) Für $i \geq 2$ ist $\deg(f_i) > \deg(f_{i+1})$ oder $f_{i+1}(X) = 0$. Der Grad von f_i erniedrigt (für $i \geq 2$) sich in jedem Schritt um (mind.) eins, der Algorithmus terminiert.
Wende wiederholt (1) an. Nach Voraussetzung ist $f_i(X) \neq 0$ für $i \leq k$ und mit (1) folgt:
 $I_{f_1, f_2} = I_{f_2, f_3} = \dots = I_{f_k, f_{k+1}} = I_{f_k, 0}$.
- (3) (a) $I_{f, g} = (X^2 + 1)\mathbf{R}[X]$.
(b) $I_{f, g} = (X^4 + 1)\mathbf{F}_5[X]$.
(c) $I_{f, g} = (X + \alpha)\mathbf{F}_4[X]$.

Aufgabe 15.

- (1) (a) $(2 + i)^4 = 24i - 7$, $(2i)^{12} = 2^{12} = 4096$.
(b) $(1 + \alpha)^4 = 1 + \alpha$, $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 1 + \alpha$.
(c) $(1 + \beta + \beta^2)\beta^2 = 1$, $\sum_{x \in \mathbf{F}_8} x = 0$.
(d) $(\iota - 1)^8 = 1$, $\prod_{x \in \mathbf{F}_9 \setminus \{0\}} x = -1$.
- (2) (a) Körper: $X^2 - 2$ in $\mathbf{Q}$ irreduzibel, da $\sqrt{2} \notin \mathbf{Q}$.
(b) Kein Körper: $X^2 - 1$ hat Nullstelle $1 \in \mathbf{R}$.
(c) Kein Körper: $X^{12} - 1$ hat Nullstelle $1 \in \mathbf{F}_2$.
(d) Körper: $X^3 + X + 1$ hat keine Nullstelle in $\mathbf{F}_5$.
- (3) (a) Mit $x + iy \neq 0$ ($x, y \in \mathbf{R}$) ist $x \neq 0$ oder $y \neq 0$ und damit ist $(x + iy)(x - iy) = x^2 - i^2y^2 = x^2 + y^2 > 0$.
(b) Der Körper K werde als $(K, +, \cdot)$ geschrieben. Dann ist $(K \setminus \{0\}, \cdot)$ eine abelsche Gruppe mit $q - 1$ Elementen. Betrachte zu einem $x \in K \setminus \{0\}$ die Menge $G_x := \{x^m \mid m \in \mathbf{Z}\}$. Dies ist eine Untergruppe von $(K \setminus \{0\}, \cdot)$, da für zwei Elemente $x^m, x^n \in G_x$ aus G_x (mit $n, m \in \mathbf{Z}$) stets $x^m \cdot (x^n)^{-1} = x^{m-n}$ wieder in G_x liegt (vgl. Aufgabe 8.(3)). Die Ordnung von x ist gleich der Anzahl der Elemente in G_x . Nach Aufgabe 4.(1) gilt: $\#G_x$ teilt $\#(K \setminus \{0\}) = q - 1$, also $z \cdot (\#G_x) = q - 1$ mit einem $z \in \mathbf{Z}$. Damit ist $x^{q-1} = (x^{\#G_x})^z = 1^z = 1$.
- (4) (a) $(1 + i)^{-1} = \frac{1-i}{2}$.
(b) $(1 + \beta^2)^{-1} = (1 + \beta^2)^6 = \beta$.
(c) $(\iota + 1)^{-1} = (\iota + 1)^7 = \iota - 1$.
(d) $(x + \alpha y)^{-1} = (x + \alpha y)^2 = x + \alpha^2 y = (x + y) + \alpha y$.