Aufgabe 1.
Zeigen Sie, dass die folgenden Polynome irreduzibel sind:

1. $3t^6 + 4t^4 - 6t^2 - 10 \in \mathbb{Z}[t]$
2. $t^3 + 39t^2 - 4t + 8 \in \mathbb{Q}[t]$
3. $2t^3 - 14t + 6 \in \mathbb{Q}[t]$
4. $t^4 + 1 \in \mathbb{Q}[t]$
5. $t^5 - u \in \mathbb{Q}(u)[t]$
6. $t^2u + tu^2 - t - u + 1 \in \mathbb{Q}[t, u]$

Aufgabe 2.
Bestimmen Sie jeweils alle Lösungen $x \in \mathbb{Z}$ der folgenden Systeme simultaner Kongruenzen:

1. $\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$
2. $\begin{cases} 5x \equiv 6 \pmod{12} \\ 3x \equiv 7 \pmod{11} \end{cases}$
3. $\begin{cases} x \equiv 10 \pmod 6 \\ x \equiv -6 \pmod{14} \end{cases}$
4. $\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv -2 \pmod{10} \\ x \equiv 1 \pmod 7 \end{cases}$

Aufgabe 3.
Bestimmen Sie mithilfe des euklidischen Algorithmus jeweils den größten gemeinsamen Teiler der folgenden Zahlen, und drücken Sie diesen als $\mathbb{Z}$-Linearkombination dieser Zahlen aus.

1. 270, 192
2. 30, 42, 70

Aufgabe 4.
Es sei R ein kommutativer Ring und $P \trianglelefteq R$ ein Primideal. Zeigen Sie, dass

$$S := R \setminus P = \{r \in R \mid r \notin P\}$$

ein multiplikative Teilmenge von R ist.

Aufgabe 5.
Zeigen Sie, dass der Ring $\mathbb{Z}[\sqrt{-2}] = \mathbb{Z}[i\sqrt{2}]$ euklidisch ist.

Aufgabe 6.
Es seien $n, m \geq 1$. Zeigen Sie, dass

$$\mathbb{Z}/n \times \mathbb{Z}/m \cong \mathbb{Z}/\mathrm{ggT}(n,m) \times \mathbb{Z}/\mathrm{kgV}(n,m)\,.$$

Aufgabe 7.
Für alle $n \geq 1$ sei $\varphi(n) = |\{1 \leq k \leq n \mid k \text{ und } n \text{ sind teilerfremd}\}|$.

1. Begründen Sie, dass $\varphi(n) = |(\mathbb{Z}/n)^\times|$ gilt.
2. Zeigen Sie, dass $\varphi(nm) = \varphi(n)\varphi(m)$ gilt, wenn $n, m \geq 1$ teilerfremd sind.
3. Zeige Sie für p prim und $\ell \geq 1$, dass $\varphi(p^\ell) = p^{\ell-1}(p-1)$ gilt.
4. Bestimmen Sie $\varphi(42)$, $\varphi(57)$ und $\varphi(144)$.

Lösungen

Lösung 3.

1. Es gilt

$$\begin{aligned} &\operatorname{ggT}(270,192) = \operatorname{ggT}(192+78,192) \\ &= \operatorname{ggT}(192,78) = \operatorname{ggT}(2\cdot 78+36,78) \\ &= \operatorname{ggT}(78,36) = \operatorname{ggT}(2\cdot 36+6,36) \\ &= \operatorname{ggT}(36,6) = 6\,. \end{aligned}$$

   Dabei gilt

$$\begin{aligned} 6 &= 78 - 2\cdot 36 = 78 - 2\cdot(192 - 2\cdot 78) \\ &= 5\cdot 78 - 2\cdot 192 = 5\cdot(270-192) - 2\cdot 192 \\ &= 5\cdot 270 - 7\cdot 192\,. \end{aligned}$$

2. Es gilt $\operatorname{ggT}(30,42,70) = \operatorname{ggT}(\operatorname{ggT}(30,42),70)$, weshalb wir wiederholt den euklidischen Algorithmus anwenden können.

   a) Es gilt

$$\begin{aligned} &\operatorname{ggT}(42,30) = \operatorname{ggT}(30+12,30) \\ &= \operatorname{ggT}(30,12) = \operatorname{ggT}(2\cdot 12+6,12) \\ &= \operatorname{ggT}(12,6) = 6\,. \end{aligned}$$

   Dabei gilt

$$6 = 30 - 2\cdot 12 = 30 - 2\cdot(42-30) = 3\cdot 30 - 2\cdot 42\,. \tag{1}$$

3. Es gilt nun

   a) Es gilt

$$\begin{aligned} &\operatorname{ggT}(70,6) = \operatorname{ggT}(11\cdot 6+4,6) \\ &= \operatorname{ggT}(6,4) = \operatorname{ggT}(4+2,4) \\ &= \operatorname{ggT}(4,2) = 2\,. \end{aligned}$$

   Dabei gilt

$$2 = 4 - 2 = 4 - (6-4) = 2\cdot 4 - 6 = 2\cdot(70 - 11\cdot 6) - 6 = 2\cdot 70 - 23\cdot 6\,.$$

   Durch Einsetzen von Gleichung (1) ergibt sich damit, dass

$$2 = 2\cdot 70 - 23\cdot(3\cdot 30 - 2\cdot 42) = 2\cdot 70 + 46\cdot 42 - 69\cdot 30\,.$$

Lösung 4.
Es gilt
$$1 \in S \iff 1 \notin P \iff P \neq R\,,$$
wobei $P \neq R$ gilt, da P prim ist. Es gilt außerdem, dass
$$\forall x, y \in R : (xy \in P \implies x \in P \vee y \in P)\,,$$
was äquivalent zu
$$\forall x, y \in R : (x \notin P \wedge y \notin P \implies xy \notin P)$$
ist, was sich wiederum zu
$$\forall x, y \in R : (x \in S \wedge y \in S \implies xy \in S)$$
umschreiben lässt. Für alle $s, t \in S$ gilt also auch $st \in S$.

Lösung 5.
Für jedes $z = a + ib\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ mit $a, b \in \mathbb{Z}$ definieren wir die *Norm* von z als $N(z) \coloneqq |z|^2 = a^2 + 2b^2 \in \mathbb{N}$. Dann ist $\mathbb{Z}[\sqrt{-2}]$ zusammen mit N ein euklidischer Ring:
Man bemerke, dass $\mathbb{Z}[\sqrt{-2}]$ in der komplexen Zahlenebene $\mathbb{C}$ ein „Gitter“ von Breite 1 und Höhe $\sqrt{2}$ bildet, weshalb es für jedes Element $z \in \mathbb{C}$ ein $w \in \mathbb{Z}[\sqrt{-2}]$ mit
$$|z - w| \leq \frac{\sqrt{1^2 + \sqrt{2}^2}}{2} = \frac{\sqrt{3}}{2} < 1$$
gibt. Für $f, g \in \mathbb{Z}[\sqrt{-2}]$ mit $g \neq 0$ lässt sich in $\mathbb{C}$ der Quotient f/g bilden, und es gibt ein $q \in \mathbb{Z}[\sqrt{-2}]$ mit $|f/g - w| < 1$ gibt. Für $r \coloneqq f - qg$ gilt dann $f = qg + r$, wobei
$$N(r) = |r|^2 = |f - qg|^2 = \underbrace{|f/g - q|^2}_{<1} |g|^2 < |g|^2 = N(g)\,.$$

Lösung 6.
Es sei $\mathcal{P} \subseteq \mathbb{N}$ die übliche Menge der Primzahlen. Aus den Primfaktorzerlegungen
$$n = \prod_{p \in \mathcal{P}} p^{\nu_p} \qquad \text{und} \qquad m = \prod_{p \in \mathcal{P}} p^{\mu_p}\,.$$
ergeben sich die Primfaktorzerlegungen
$$\operatorname{ggT}(n, m) = \prod_{p \in \mathcal{P}} p^{\min(\nu_p, \mu_p)} \qquad \text{und} \qquad \operatorname{kgV}(n, m) = \prod_{p \in \mathcal{P}} p^{\max(\nu_p, \mu_p)}\,.$$

Nach dem chinesischen Restklassensatze gelten deshalb

$$\begin{aligned}\mathbb{Z}/n &\cong \prod_{p\in\mathcal{P}} \mathbb{Z}/p^{\nu_p}\,,\\ \mathbb{Z}/m &\cong \prod_{p\in\mathcal{P}} \mathbb{Z}/p^{\mu_p}\,,\\ \mathbb{Z}/\operatorname{ggT}(n,m) &\cong \prod_{p\in\mathcal{P}} \mathbb{Z}/p^{\min(\nu_p,\mu_p)}\,,\\ \mathbb{Z}/\operatorname{kgV}(n,m) &\cong \prod_{p\in\mathcal{P}} \mathbb{Z}/p^{\max(\nu_p,\mu_p)}\,,\end{aligned}$$

und somit

$$\begin{aligned}\mathbb{Z}/n\times\mathbb{Z}/m &\cong \prod_{p\in\mathcal{P}} (\mathbb{Z}/p^{\nu_p}\times\mathbb{Z}/p^{\mu_p})\,,\\ \mathbb{Z}/\operatorname{ggT}(n,m)\times\mathbb{Z}/\operatorname{kgV}(n,m) &\cong \prod_{p\in\mathcal{P}} \left(\mathbb{Z}/p^{\min(\nu_p,\mu_p)}\times\mathbb{Z}/p^{\max(\nu_p,\mu_p)}\right)\,.\end{aligned}$$

Dabei gilt für jedes $p\in\mathcal{P}$, dass

$$\mathbb{Z}/p^{\nu_p}\times\mathbb{Z}/p^{\mu_p}\cong\mathbb{Z}/p^{\min(\nu_p,\mu_p)}\times\mathbb{Z}/p^{\max(\nu_p,\mu_p)}\,,$$

denn es gilt

$$\{\nu_p,\mu_p\}=\{\min(\nu_p,\mu_p),\max(\nu_p,\mu_p)\}\,.$$

Lösung 7.

1. Es ist $\overline{k}\in\mathbb{Z}/n$ genau dann eine Einheit, wenn k und n teilerfremd sind. Dies ergibt sich etwa dadurch, dass

$$\begin{aligned}&\overline{k}\in(\mathbb{Z}/n)^\times\\ \iff{}&\exists\overline{a}\in\mathbb{Z}/n:\overline{a}\cdot\overline{k}=\overline{1}\\ \iff{}&\exists\overline{a}\in\mathbb{Z}/n:\overline{ak}=\overline{1}\\ \iff{}&\exists a,b\in\mathbb{Z}:ak+bn=1\\ \iff{}&1\in(k,n)=(\operatorname{ggT}(k,n))\\ \iff{}&\operatorname{ggT}(k,n)\text{ ist eine Einheit}\,.\end{aligned}$$

   Es gilt somit

$$\begin{aligned}|(\mathbb{Z}/n)^\times| &= |\{1\leq k\leq n\,|\,\overline{k}\text{ ist eine Einheit in }\mathbb{Z}/n\}|\\ &= |\{1\leq k\leq n\,|\,k\text{ und }n\text{ sind teilerfremd}\}|=\varphi(n)\,.\end{aligned}$$

2. Nach dem chinesischen Restklassensatz gilt $\mathbb{Z}/(nm)=\mathbb{Z}/n\times\mathbb{Z}/m$, und somit

$$\begin{aligned}\varphi(nm) &= \left|(\mathbb{Z}/(nm))^\times\right| = \left|(\mathbb{Z}/n\times\mathbb{Z}/m)^\times\right|\\ &= \left|(\mathbb{Z}/n)^\times\times(\mathbb{Z}/m)^\times\right| = \left|(\mathbb{Z}/n)^\times\right|\left|(\mathbb{Z}/m)^\times\right| = \varphi(n)\varphi(m)\,.\end{aligned}$$

3. Es ist $1 \leq k \leq p^\ell$ genau dann teilerfremd zu p^ℓ, wenn k den Primfaktor p nicht enthält. Da jede p-te Zahl durch p teilbar ist, gilt somit

$$\varphi(p^\ell) = p^\ell - \frac{p^\ell}{p} = p^\ell - p^{\ell-1} = p^{\ell-1}(p-1)\,.$$

4. Es gelten

$$\begin{aligned}
\varphi(42) &= \varphi(2 \cdot 3 \cdot 7) = \varphi(2)\varphi(3)\varphi(7) = 1 \cdot 2 \cdot 6 = 12\,,\\
\varphi(57) &= \varphi(3 \cdot 19) = \varphi(3)\varphi(19) = 2 \cdot 18 = 36\,,\\
\varphi(144) &= \varphi(2^4 \cdot 3^2) = \varphi(2^4)\varphi(3^2) = 2^3 \cdot 1 \cdot 3^1 \cdot 2 = 48\,.
\end{aligned}$$