Konvention. In Aufgabenstellungen getätigte Aussagen sind jeweils zu beweisen, auch wenn kein explizites „Zeigen Sie, dass ...“ dabeisteht.

1. Sei $(R, +, \cdot)$ ein Ring, $a_1, \dots a_n$, $b_1, \dots b_m \in R$, dann gilt
$$\left(\sum_{i=1}^{n} a_i\right) \cdot \left(\sum_{j=1}^{m} b_j\right) = \sum_{\substack{1 \le i \le n \\ 1 \le j \le m}} a_i \cdot b_j.$$

2. Sei R ein Ring; $a \neq 0$ heiße Links-Nullteiler, wenn $\exists b \in R$ mit $b \neq 0$ und $a \cdot b = 0$. Dann ist für $a \in R$ ist äquivalent:
   (a) a ist links kürzbar (d. h. $\forall b, c \in R : a \cdot b = a \cdot c \to b = c$).
   (b) a ist kein Links-Nullteiler.
   (c) $L_a \colon R \to R$, $L_a(x) = a \cdot x$ ist injektiv.

   Außerdem ist (in einem Ring mit Eins) jede Linkseinheit (a heißt Linkseinheit, wenn es ein $b \in R$ mit $a \cdot b = 1_R$ gibt) links kürzbar.

3. Sei $(R, +, \cdot)$ ein Ring, N_l die Menge der Links-Nullteiler, N_r die Menge der Rechts-Nullteiler und $N = N_l \cup N_r$ die Menge der Nullteiler in R. Zeigen Sie
   (b) $R \setminus N_r$, $R \setminus N_l$ und $R \setminus N$ sind bzgl. $\cdot$ abgeschlossen.
   (c) $r \in R$, $a \in N_r \implies a \cdot r \in N_r$,
   (d) $r \in R$, $a \in N_l \implies r \cdot a \in N_l$.

4. Bestimmen Sie alle Einheiten des Rings $\mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}$ für
   (a) $D < 0$
   (b) $D = 3$.
   Hinweis. $2 + \sqrt{3}$.

5. Sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins. Ein $a \in R$ heißt *idempotent*, wenn $a^2 = a$. Zeigen Sie, dass
   (a) a idempotent $\Rightarrow \forall n \in \mathbb{N} : a^n = a$.
   (b) a idempotent und $a \neq 1_R \Rightarrow a$ Nullteiler.
   (c) a, b idempotent $\Rightarrow ab$ idempotent.
   (d) a idempotent $\Rightarrow 1_R - a$ idempotent.

6. Sei $(R, +, \cdot)$ ein Ring, $\mathrm{Nil}(R) = \{a \in R \mid \exists n \in \mathbb{N} : a^n = 0\}$ die Menge der nilpotenten Elemente von R. Wenn R kommutativ ist, dann ist $\mathrm{Nil}(R)$ ein Ideal von R.

7. Sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins, $E(R)$ die Menge der invertierbaren Elemente (Einheiten) von R, und a, $b \in R$. Dann gilt:
   (a) $a \in E(R)$, $b \in \mathrm{Nil}(R) \implies a - b$, $a + b \in E(R)$
   (b) $1_R - b \in \mathrm{Nil}(R) \implies b \in E(R)$.

8. Sei I_λ, $\lambda \in \Lambda$ eine Familie von Idealen, für die
$$\forall \lambda, \mu \in \Lambda : I_\lambda \subseteq I_\mu \text{ oder } I_\mu \subseteq I_\lambda$$
   gilt, dann ist
$$\bigcup_{\lambda \in \Lambda} I_\lambda \trianglelefteq R.$$

9. Sei $I \neq \emptyset$ eine Indexmenge und R_i seien Ringe für alle $i \in I$. Sei $(\prod_{i\in I} R_i, +)$ das direkte Produkt der Gruppen $(R_i, +)$.

   (a) Zeigen Sie, dass $\prod_{i\in I} R_i$ bezüglich der Multiplikation $(r_i)_{i\in I} \cdot (s_i)_{i\in I} = (r_i \cdot s_i)_{i\in I}$ ein Ring ist.

   (b) Dieser Ring ist genau dann ein Ring mit Eins bzw. kommutativ, wenn für alle $i \in I$ die Ringe R_i Ringe mit Eins bzw. kommutativ sind.

   (c) Die kanonischen Projektionen $\pi_j : \prod_{i\in I} R_i \longrightarrow R_j$ mit $\pi_j((r_i)_{i\in I}) = r_j$ sind Epimorphismen.
   Die kanonischen Einbettungen $\epsilon_j : R_j \longrightarrow \prod_{i\in I} R_i$ mit

   $$\epsilon_j(r) = (r_i)_{i\in I} \begin{cases} r_i = 0 & i \neq j \\ r_i = r & i = j \end{cases}$$

   sind Monomorphismen.

   (d) (*Universelle Eigenschaft des direkten Produkts von Ringen*)
   Sei $\{R_i \mid i \in I\}$ eine Familie von Ringen und S ein Ring.
   Weiters sei $\{\phi_i : S \to R_i\}$ eine Familie von Ringhomomorphismen.
   Zeigen Sie, dass dann genau ein Ringhomomorphismus $\varphi : S \to \prod_{i\in I} R_i$ existiert, sodass für alle $i \in I$ gilt: $\pi_i \circ \varphi = \varphi_i$.

10. Sei R ein kommutativer Ring und $\emptyset \neq S \subseteq R$ eine multiplikativ abgeschlossene Menge.

    (a) Die auf $R \times S$ durch

    $$(r,\, s) \sim (r',\, s') \iff \exists t \in S \;\; t(rs' - r's) = 0$$

    definierte Relation ist eine Äquivalenzrelation.

    (b) Wir bezeichnen die Äquivalenzklasse von $(r,\, s)$ bzgl. $\sim$ mit $\frac{r}{s}$ und mit $S^{-1}R$ die Menge $R \times S/_\sim$ der Äquivalenzklassen in $R \times S$ bzgl. $\sim$. Zeigen Sie:
    Für beliebige $s,\, t \in S$ und $r \in R$ gilt

    $$\frac{r}{s} = \frac{rt}{st} \qquad \frac{s}{s} = \frac{t}{t} \qquad \frac{0}{s} = \frac{0}{t}$$

    (c) Wenn $0 \in S$, dann ist $S^{-1}R = \{\frac{0}{s} \mid s \in S\}$, also $|S^{-1}R| = 1$.

    (d) Durch $(a, b) + (c, d) := (ad + bc, bd)$ und $(a, b) \cdot (c, d) := (ac, bd)$ sind auf $S^{-1}R$ zwei Operationen definiert. Damit wird $(S^{-1}R, +, \cdot)$ ein kommutativer Ring mit 1.

    Sei ab jetzt R ein Integritätsbereich.

    (e) $Q(R) := (R \setminus \{0\})^{-1}R$ ist mit diesen Operationen ein Körper.

    (f) $\iota : R \to Q(R); a \mapsto (a, 1)$ ist ein Monomorphismus.

    (g) $Q(R)$ hat die universelle Eigenschaft von Quotientenkörpern. (Für jeden Körper K und jeden Monomorphismus $\varphi : R \to K$ gibt es einen Monomorphismus $\Phi : Q(R) \to K$ mit $\Phi \circ \iota = \varphi$.)

11. Geben Sie alle Einheiten, Nullteiler, irreduziblen Elemente und Primelemente von $\mathbb{Z}/6\mathbb{Z}$ an. Was fällt auf?

12. Sei $D \in \mathbb{Z}$, D kein Quadrat. Betrachte die Abbildung („Norm“)

$$N : \mathbb{Q}[\sqrt{D}] \to \mathbb{Q} : a + b\sqrt{D} \mapsto a^2 - Db^2.$$

    (a) Zeigen Sie, dass N mit der Multiplikation verträglich (d.h. ein Monoidhomomorphismus) ist, d.h.,
    $$\forall \alpha, \beta \in \mathbb{Q}[\sqrt{D}] : N(\alpha \cdot \beta) = N(\alpha)N(\beta),$$
    der $N(\mathbb{Z}[\sqrt{D}]) \subseteq \mathbb{Z}$ erfüllt.
    Wie verhält sich N zu einer bekannten Funktion (welcher?) von $\mathbb{C}$ nach $\mathbb{R}$, falls $D < 0$?

    (b) Seien α, $\beta \in \mathbb{Z}[\sqrt{D}]$. Zeigen Sie, dass $N(\alpha) \mid N(\beta)$, falls $\alpha \mid \beta$.

    (c) Sei $\alpha \in \mathbb{Z}[\sqrt{D}]$. Zeigen Sie, dass α genau dann eine Einheit ist, wenn $N(\alpha) \in \{\pm 1\}$.

13. Sei $R = \mathbb{Z}[\sqrt{10}]$. Zeigen Sie:

    (a) 2, 3, $4 + \sqrt{10}$ und $4 - \sqrt{10}$ sind irreduzibel.

    (b) 2, 3, $4 + \sqrt{10}$ und $4 - \sqrt{10}$ sind nicht prim.

    (c) R ist kein faktorieller Ring; zeigen Sie insbesondere, dass 6 zwei wesentlich verschiedene Zerlegungen in irreduzible Elemente besitzt.

14. Sei R ein Ring, $a \in R$, und A, B, C Teilmengen von R. Dann gilt

    (a) $A + (B + C) = (A + B) + C$

    (b) $A(BC) = (AB)C$

    (c) $A \leq R$ und $B \trianglelefteq R$, dann gilt $A + B \leq R$

    (d) wenn $A \trianglelefteq R$ und $B \trianglelefteq R$, dann auch $A + B \trianglelefteq R$ und $AB \trianglelefteq R$

    (e) wenn $A \trianglelefteq R$ und R ein Einselement hat, dann gilt $RA = AR = A$

    (f) B bzgl. + abgeschlossen $\implies$ $aB = \{a \cdot b \mid b \in B\}$ und $Ba = \{b \cdot a \mid b \in B\}$ sind bzgl. + abgeschlossen.

    (g) $A \leq R$ und $B \trianglelefteq R$, dann gilt $A \cap B \trianglelefteq A$.

    Hier werden die üblichen Definitionen für Komplexprodukte

$$M + N = \{m + n \mid m \in M, n \in N\},$$
$$M \cdot N = \{m_1 n_1 + \ldots + m_r n_r \mid r \in \mathbb{N}_0, m_j \in M, n_j \in N\}$$

    verwendet.

15. Seien R ein kommutativer Ring und I, J Ideale von R. Dann gilt $IJ \subseteq I \cap J$.

16. Sei R ein kommutativer Ring mit Eins, $M \lhd R$. M ist genau dann maximal, wenn es für alle $r \in R \setminus M$ ein $s \in R$ gibt, sodass $1 - rs \in M$.

17. Sei K ein Körper, dann hat $M_n(K)$, der Ring der $n \times n$ Matrizen über K, keine Ideale außer $\{0\}$ und $M_n(K)$.

    (Hinweis: Multiplikation von $A \in M_n(K)$ (nicht die Null-Matrix) mit E_{ij} von links und E_{kl} von rechts, wobei E_{ij} die Matrix mit der Eintragung 1 an der Stelle (i, j) und 0 sonst bezeichnet).

18. Sei R ein ZPE-Ring und $\mathcal{P}$ ein Repräsentantensystem der Primelemente von R bezüglich Assoziiertheit. Für $a \in R$ und $p \in \mathcal{P}$ setze

$$v_p(a) := \max\{k \in \mathbb{N}_0 : p^k \mid a\},$$

insbesondere $v_p(0) = \infty$ für alle $p \in \mathcal{P}$. Zeigen Sie, dass für $a, b \in R$ gilt:

(a) Falls $a \neq 0$, so gilt

$$a = u_a \prod_{\substack{p \in \mathcal{P} \\ p \mid a}} p^{v_p(a)},$$

wobei $u_a \in \mathcal{E}(R)$.

(b) $a \mid b \iff \forall p \in \mathcal{P} : v_p(a) \leq v_p(b)$,

(c) $\forall p \in \mathcal{P} : v_p(a \cdot b) = v_p(a) + v_p(b)$,

(d) $a \sim b \iff \forall p \in \mathcal{P} : v_p(a) = v_p(b)$,

(e) $\forall p \in \mathcal{P} : v_p(\mathrm{ggT}(a, b)) = \min(v_p(a), v_p(b))$,

(f) $\forall p \in \mathcal{P} : v_p(\mathrm{kgV}(a, b)) = \max(v_p(a), v_p(b))$,

(g) $\forall p \in \mathcal{P} : v_p(a + b) \geq \min(v_p(a), v_p(b))$,

(h) $\forall p \in \mathcal{P} : v_p(a) \neq v_p(b) \to v_p(a + b) = \min(v_p(a), v_p(b))$,

(i) $(R, \cdot) \simeq \mathcal{E}(R) \times \sum_{p \in \mathcal{P}} \mathbb{N}_0$ (Isomorphismus von Monoiden und direktes Produkt bzw. Summe von Monoiden sind analog wie Isomorphismen von Gruppen und direktes Produkt bzw. Summe definiert, das Wort „Gruppe“ ist jeweils durch „Monoid“ zu ersetzen.)

(j) Für $p \in \mathcal{P}$ definiere den p-adischen Absolutbetrag durch $|x|_p := p^{-v_p(x)}$. Zeigen Sie, dass dann $(R, \| \cdot |)$ ein metrischer Raum ist.

19. Sei R ein ZPE-Ring und $a, b, d \in R \setminus \{0\}$. a und b seien teilerfremd. Dann gilt

(a) $a \mid bd \Rightarrow a \mid d$

(b) $a \mid d \wedge b \mid d \Rightarrow ab \mid d$

(c) $a \mid b^2 \Rightarrow a \in \mathcal{E}(R)$

20. Sei R ein kommutativer Ring mit Eins, x eine Unbestimmte über R und $a \in R$. Für $f \in R[x]$ mit $\deg f \geq 1$ sei $f_a := f(x + a) \in R[x]$.

Dann ist f genau dann irreduzibel, wenn f_a irreduzibel ist.

21. Sei K ein Körper und $f \in K[x]$ mit $2 \leq \deg f \leq 3$. Dann ist f genau dann irreduzibel, wenn für alle $\alpha \in K$ $f(\alpha) \neq 0$.

Gilt diese Aussage auch, wenn $\deg f = 4$?

22. Sei R ein faktorieller Ring, $f \in R[X]$ mit $f = \sum_{j=0}^{d} a_j X^j$, $a_d \neq 0$, und Q der Quotientenkörper von R.

(a) Sei $r/s \in Q$ eine Nullstelle von f mit $\mathrm{ggT}(r, s) = 1$. Zeigen Sie, dass $r \mid a_0$ und $s \mid a_d$.

(b) Sei f normiert (d.h., $a_d = 1$) und $\alpha \in Q$ eine Nullstelle von f in Q. Zeigen Sie, dass dann sogar $\alpha \in R$ gilt.

(c) Sei $g = \sum_{j=0}^{d} a_j a_d^{d-1-j} X^j$ und $\alpha \in Q$. Dann ist $g \in R[X]$ normiert und α genau dann eine Nullstelle von f, wenn $a_d \alpha$ eine Nullstelle von g ist.

(d) Sei α eine Nullstelle von f. Dann gibt es ein $b \in R$ mit $b \mid a_d^{d-1} a_0$ und $\alpha = b/a_d$.

23. *Eisensteinsches Irreduzibilitätskriterium.* Sei R ein Integritätsring und $f = \sum_{i=0}^{n} a_i X^i$ ein primitives Polynom aus $R[X]$ vom Grad $n > 0$. Gibt es ein Primelement p von R mit

$$p \mid a_i \text{ für } i \in \{0, \ldots, n-1\}, \qquad p \nmid a_n, \qquad p^2 \nmid a_0,$$

dann ist f irreduzibel in $R[X]$.

24. Sei R ein Körper, $n \in \mathbb{N}$, $a_0, \ldots, a_n$, $b_0, \ldots, b_n \in R$ mit paarweise verschiedenen a_i. Zeigen Sie *unter Verwendung des Chinesischen Restsatzes*, dass es genau ein Polynom $f \in R[X]$ mit $\deg f \leq n$ und $f(a_i) = b_i$ für $i = 0, \ldots, n$ gibt.

25. Lösen Sie das System

$$\begin{aligned} 3x &\equiv 1 \mod 9 \\ x &\equiv 6 \mod 13 \\ 7x &\equiv 5 \mod 56. \end{aligned}$$

26. Bestimmen Sie die kleinste positive ganze Zahl x mit

$$x \equiv 28 \pmod{49},$$
$$x \equiv 15 \pmod{41}.$$

27. Zeigen Sie: Für alle zu 561 teilerfremden Zahlen a gilt

$$a^{560} \equiv 1 \pmod{561}.$$

28. Wir definieren $\lambda : \mathbb{N} \to \mathbb{N}$ durch

$$\begin{aligned} \lambda(p^\alpha) &= \varphi(p^\alpha) = (p-1)p^{\alpha-1}, && p \text{ ungerade Primzahl, } \alpha \geq 1, \\ \lambda(2^\alpha) &= \varphi(2^\alpha)/2 = 2^{\alpha-2}, && \alpha \geq 3, \\ \lambda(4) &= 2, \\ \lambda(2) &= 1, \end{aligned}$$

und für verschiedene Primzahlen $p_1, \ldots, p_r$ und natürliche Zahlen $\alpha_1, \ldots, \alpha_r$

$$\lambda(p_1^{\alpha_1} \ldots p_r^{\alpha_r}) = \mathrm{kgV}(\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_r^{\alpha_r})).$$

Zeigen Sie unter Verwendung der Zerlegung von $\mathcal{E}(\mathbb{Z}/m\mathbb{Z})$ in ein Produkt zyklischer Gruppen, dass für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$

$$a^{\lambda(m)} \equiv 1 \pmod{m}$$

gilt. Zeigen Sie weiters, dass diese Eigenschaften für keinen kleineren Exponenten k an der Stelle von $\lambda(m)$ gilt.

29. Es sei K ein Körper der Charakteristik p, p prim. Dann gilt für $a, b \in K$ und für alle $k \in \mathbb{N}_0$

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}.$$

30. Bestimmen Sie den größten gemeinsamen Teiler von $f = x^8 + 2x^5 + x^3 + x^2 + 1$ und $g = 2x^6 + x^5 + 2x^3 + 2x^2 + 2$ über $\mathbb{Z}/3\mathbb{Z}$.

31. $f = x^4 + 1$ ist prim in $\mathbb{Z}[x]$.

32. $f = x^2 + x + 1$ ist irreduzibel in $\mathbb{Z}_2[x]$ (wobei wie üblich $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$).

33. Eine über $\mathbb{Q}$ algebraische Zahl α heißt *ganzalgebraisch*, wenn es ein normiertes Polynom $f \in \mathbb{Z}[X]$ mit $f(\alpha) = 0$ gibt. Zeigen Sie, dass dann das Minimalpolynom von α über $\mathbb{Q}$ in $\mathbb{Z}[X]$ liegt.

34. Bestimmen Sie den Zerfällungskörper K des Polynoms $X^3 - 2X^2 - 5X - 1$ über $\mathbb{Q}$. Geben Sie den Grad $[K : \mathbb{Q}]$ an.

35. Man berechne das Minimalpolynom von $\sqrt{2} + \sqrt{3}$ über $\mathbb{Q}$.

36. Sei F ein Körper und $G \leq \mathrm{Aut}(F)$, dann bilden die Elemente von $\mathrm{Fix}_G(F)$ tatsächlich einen Körper. Dabei ist $\mathrm{Aut}(F) := \{\psi : F \to F \text{ Automorphismus}\}$, $\mathrm{Fix}_G(F) := \{a \in F : \psi(a) = a \text{ für alle } \psi \in G\}$.

37. *Vandermonde-Determinante.* Sei R ein faktorieller Ring, $X_1, \ldots, X_n$ Unbestimmte über R. Beweisen Sie ohne Induktion:

$$\det \begin{pmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_n \\ X_1^2 & X_2^2 & \ldots & X_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \ldots & X_n^{n-1} \end{pmatrix} = \prod_{1 \le i < j \le n} (X_j - X_i).$$

Hinweis. Polynom, Nullstellen, Grade, 1 einfacher Koeffizientenvergleich.

38. Sei L eine algebraische Körpererweiterung von K und α, $\beta \in L$ zwei Elemente, deren Grade n bzw. m über K teilerfremd seien. Man beweise: $[K(\alpha, \beta) : K] = mn$.

39. Sei K ein Körper und α ein Element, das eine Körpererweiterung von K von Grad 5 erzeugt. Man beweise, dass α^2 dieselbe Erweiterung erzeugt.

40. Man zerlege $X^9 - X$ und $X^{27} - X$ über $\mathbb{F}_3$ in irreduzible Faktoren.

41. Bestimmen Sie ein Polynom $p(X) \in \mathbb{F}_2[X]$, sodass $\mathbb{F}_{32} \cong \mathbb{F}_2[X]/(p(X))$, und ein primitives Element dieses Körpers.

42. Sei F/K eine Körpererweiterung und $f \in K[x]$, dann bildet ein $\psi \in \mathrm{Aut}_K(F)$ Wurzeln von f wiederum auf Wurzeln ab. Dabei ist

$$\mathrm{Aut}_K(F) := \{\psi : F \to F \text{ Automorphismus mit } \psi|_K = \mathrm{id}_K\}.$$

43. Sei K ein Körper, $k \in \mathbb{N}$, $\ell \in \mathbb{N}_0$. Zeigen Sie, dass $X^k - X$ das Polynom $X^{k^\ell} - X$ in $K[X]$ teilt.

44. Sei K ein Körper, $n \in \mathbb{N}$ mit $\chi(K) \nmid n$, $E_n(K)$ die Menge der n-ten Einheitswurzeln. Das Polynom $X^n - 1$ zerfalle in $K[X]$ in Linearfaktoren. Zeigen Sie, dass dann

$$\sum_{\zeta \in E_n(K)} \zeta = \begin{cases} 1, & \text{wenn } n = 1, \\ 0, & \text{sonst} \end{cases}$$

gilt.

45. Zeigen Sie, dass $\overline{\mathbb{Q}} := \{z \in \mathbb{C} : z \text{ algebraisch über } \mathbb{Q}\}$ ein algebraisch abgeschlossener Körper ist. (Ein Körper K heißt algebraisch abgeschlossen, wenn jedes über K algebraische Element bereits ein Element von K ist.)

46. Zeigen Sie: Wenn es modulo m eine Primitivwurzel gibt, so gibt es $\varphi(\varphi(m))$ Primitivwurzeln modulo m.

47. Geben Sie eine explizite Formel für $\cos(2\pi/5)$ an.

48. Es sei $f \in \mathbb{Z}[X]$ normiert mit Nullstellen $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, sodass $\alpha_1 > 1$ und $0 < |\alpha_2|, \ldots, |\alpha_n| < 1$. Dann ist f irreduzibel über $\mathbb{Q}$. (In diesem Fall nennt man α_1 eine *Pisot-Zahl*.)