Aufgabe	A1	A2	A3	A4	A5	$\sum$
Punkte						

Aufgabe 1. (a) Mit dem euklidischen Algorithmus folgt

$$X^3 - 3 = X(X^2 - 4) + 4X - 3$$
$$X^2 - 4 = \left(\frac{1}{4}X + \frac{3}{16}\right)(4X - 3) + \frac{53}{16}.$$

Da $\deg(\frac{53}{16}) = 0$ folgt bereits $\mathrm{ggT}(X^3 - 3, X^2 - 4) = 1$ in $\mathbb{Q}[X]$.

(b) Mit dem euklidischen Algorithmus folgt

$$X^3 - 3 = X^3 + 2 = X(X^2 + 1) + 4X + 2$$
$$X^2 - 4 = X^2 + 1 = (4X + 3)(4X + 2) + 0.$$

Also folgt $\mathrm{ggT}(X^3 - 3, X^2 - 4) = 4X + 2$ in $\mathbb{F}_5[X]$.

(c) Beh.: $K[X]$ hat unendlich viele normierte irreduzible Polynome.

Beweis. $X \in K[X]$ ist stets irreduzibel, es ex. also mindestens ein irreduzibles normiertes Polynom. Ang. es existieren nur $n \in \mathbb{N}$ viele normierte, irreduzible Polynome $f_1, \ldots, f_n$. Dann definiere

$$g \coloneqq f_1 \cdot \ldots \cdot f_n + 1.$$

Da $X \in K[X]$ irreduzibel, normiert ist $\deg(f_1 \cdot \ldots \cdot f_n) \geq 1$, also $\deg(g) \geq 1$. Da $K[X]$ faktoriell, ex. p irreduzibel, normiert, s.d. $p \mid g$. Dann ist aber $p \in \{f_1, \ldots, f_n\}$, also auch $p \mid f_1 \cdot \ldots \cdot f_n$. Damit folgt

$$p \mid (g - f_1 \cdot \ldots \cdot f_n) = 1.$$

Es ist also $p \in K[X]^\times$, also nicht irreduzibel ↯. □

(d) Seien $f \in K[X] \setminus \{0\}$ und $L \coloneqq K[X]/(f)$.
Beh.: Jede Restklasse $\overline{g} \in L$ hat einen eindeutigen Repräsentanten $g \in K[X]$ mit $\deg(g) < \deg(f)$.

Beweis. (i) Existenz: Sei $\overline{g} \in L$. Da $K[X]$ euklidisch und $f \neq 0$, ex. $q, r \in K[X]$ mit

$$g = qf + r.$$

mit $\deg(r) < \deg(f)$ oder $r = 0$. Da $\deg(f) \geq 0$ ist auch für $r = 0$, $\deg(r) = -\infty < 0 \leq \deg(f)$. Außerdem ist

$$\overline{g} = g + (f) = r + qf + (f) = r + (f) = \overline{r}.$$

(ii) Eindeutigkeit: Seien $r, r' \in \overline{g}$ mit $\overline{r} = \overline{r'} = \overline{g}$ und $\deg(r), \deg(r') < \deg(f)$. Dann ist $r - r' \in (f)$, also $\exists h \in K[X]$ mit $r - r' = hf$. Ang. $h \neq 0$. Dann ist $\deg(hf) \geq \deg(f)$, also $\deg(r - r') \geq \deg(f)$, aber $\deg(r), \deg(r') < \deg(f)$ ↯. Also folgt $h = 0$ und damit $r = r'$.

□

Beh.: $\dim_K L = \deg(f)$.

Beweis. Sei $\mathcal{B} = \{\overline{1}, \overline{X}, \overline{X^2}, \ldots, \overline{X^{n-1}}\}$. Dann ist $\mathcal{B}$ eine Basis von L über K, denn wegen der Eindeutigkeit der Vertreter ist $\mathcal{B}$ linear unabhängig. Außerdem ex. für $\overline{g} \in L$ ein $\overline{r} \in K[X]$ mit $\deg(r) = k \leq n - 1$, s.d. $\overline{g} = \overline{r}$ und $r = a_0 + a_1 X^1 + \ldots + a_{n-1} X^{n-1}$ für $a_0, \ldots, a_{n-1} \in K$. Dann ist

$$\overline{g} = \overline{r} = a_0\overline{1} + a_1\overline{X^1} + \ldots + a_{n-1}\overline{X^{n-1}}.$$

Also $\overline{g} \in \mathrm{Lin}(\mathcal{B})$. □

Beh.: Für $\deg(f) \geq 1$ ist $\overline{X} \in L$ Nullstelle von $f \in K[X] \subseteq L[X]$.

Beweis. Es ist $n \geq 1$, damit folgt für $a_0, \ldots, a_n \in K$:

$$f(\overline{X}) = a_n\overline{X^n} + \ldots + a_1\overline{X} + a_0 = a_nX^n + \ldots + a_1X + a_0 + (f) = f + (f) = \overline{0}.$$

□

Aufgabe 2. (a) Beh.: $f = X^3 + 2X^2 - 20 \in Q[X]$ ist irreduzibel.

Beweis. Betrachte Reduktion für $p = 3$:

$$\begin{aligned} \phi(f) &= X^3 + 2X^2 + 1 \in \mathbb{Z}/3\mathbb{Z}[X] \\ \phi(f)(0) &= 1 \\ \phi(f)(1) &= 1 \\ \phi(f)(2) &= 2. \end{aligned}$$

Falls $\phi(f)$ reduzibel, hätte einer der Teiler Grad 1, aber $\phi(f)$ hat keine Nullstelle in $\mathbb{Z}/3\mathbb{Z}$. Damit ist $\phi(f)$ irreduzibel in $\mathbb{Z}/3\mathbb{Z}[X]$ und nach Reduktionskriterium f irreduzibel in $\mathbb{Q}[X]$. □

(b) Beh.: $f = X^6 + X^3 + 1 \in \mathbb{Q}[X]$ ist irreduzibel.

Beweis. Es ist $f = f(X)$ irreduzibel $\iff$ $f(X+1)$ irreduzibel. Betrachte

$$\begin{aligned} f(X+1) &= (X+1)^6 + (X+1)^3 + 1 \\ &= X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3. \end{aligned}$$

$f(X+1)$ ist normiert, insbesondere primitiv und damit irreduzibel nach Eisenstein mit $p = 3$. Also auch $f(X)$ irreduzibel. □

(c) Beh.: $f = X^7 + 2X^5Y + 3XY^3 + 4Y^3 + 5XY + 6X \in \mathbb{C}[X, Y]$ ist irreduzibel.

Beweis. Betrachte $R \coloneqq \mathbb{C}[X]$ mit $p = X$. Dann ist

$$f = Y^3(3X + 4) + Y(2X^5 + 5X) + 1 \cdot (6X + X^7) \in R[Y].$$

Es ist $X \nmid (3X + 4)$ und $X \mid (2X^5 + 5X), X \mid (6X + X^7)$ und $X^2 \nmid (6X + X^7)$. Weiter ist f primitiv, denn $3X + 4$ ist irreduzibel. Ang.: $\mathrm{ggT}(3X + 4, 2X^5 + 5X, 6X + X^7) \neq 1$. Da R faktoriell nach Gauß, folgt $(3X + 4) \mid (2X^5 + 5X)$, aber $3X + 4 = 0 \iff X = -\frac{4}{3}$ und $2\left(-\frac{4}{3}\right)^5 + 5\left(-\frac{4}{3}\right) < 0$ ↯.
Damit ist f irreduzibel nach Eisenstein mit $p = X$ über $R[Y] = \mathbb{C}[X, Y]$. □

Aufgabe 3. (a) Seien $a, b, c \in R$ mit $a \mid bc$ und $\mathrm{ggT}(a, b) = 1$. Beh.: $a \mid c$.

Beweis. Sei p Primelement in R beliebig. Z.z.: $v_p(c) \geq v_p(a)$. Da $a \mid bc$ ex. ein $k \in R$, s.d. $bc = ka$. Da R faktoriell ist die Primfaktorzerlegung eindeutig, also folgt

$$v_p(b) + v_p(c) = \underbrace{v_p(k)}_{\geq 0} + v_p(a) \implies v_p(c) \geq v_p(a) - v_p(b).$$

Da $\mathrm{ggT}(a, b) = 1$ ist $\min(v_p(a), v_p(b)) = 0$. Falls $v_p(a) > 0$, ist also $v_p(b) = 0$, also $v_p(c) \geq v_p(a)$. Falls $v_p(a) = 0$ ist trivialerweise $v_p(c) \geq v_p(a)$. Da p beliebig, folgt $a \mid c$. □

(b) Sei $f \in R[X]$ normiert und $\alpha \in K$ Nullstelle von f. Beh.: $\alpha \in R$ und $\alpha \mid a_0$.

Beweis. Es ist $\alpha \in Q(R)[X]$, also ex. $u, v \in R$ mit $v \neq 0$ und $\mathrm{ggT}(u, v) = 1$, s.d. $\alpha = \frac{u}{v}$. Betrachte nun

$$0 = f(\alpha) = \left(\frac{u}{v}\right)^n + a_{n-1}\left(\frac{u}{v}\right)^{n-1} + \ldots + a_1\frac{u}{v} + a_0$$

Da $v \neq 0$ multipliziere mit v^n. Damit folgt

$$\begin{aligned} u^n &= -a_{n-1}u^{n-1}v - \ldots - a_1 v^{n-1}u - a_0 v^n \\ &= v(-a_{n-1}u^{n-1} - \ldots - a_1 v^{n-2}u - a_0 v^{n-1}). \end{aligned}$$

Also folgt $v \mid u^n = uu^{n-1}$. Da $\mathrm{ggT}(u,v) = 1$ folgt mit (a), dass $v \mid u^{n-1}$. Wiederholen dieses Arguments ergibt $v \mid u$. Es ex. also ein $k \in R$, s.d. $u = vk$ also $\alpha = \frac{vk}{k} = \frac{k}{1} \in R$.

Weiter ist

$$\begin{aligned} &\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0 \\ \Longrightarrow\ &\alpha(-\alpha^{n-1} - a_{n-1}\alpha^{n-2} - \ldots - a_1) = a_0. \end{aligned}$$

Also folgt $\alpha \mid a_0$. □

(c) Beh.: $X^3 + aX^2 + bX + 1 \in \mathbb{Z}[X]$ ist genau dann irreduzibel in $\mathbb{Z}[X]$ wenn $a \neq b$ und $a + b \neq -2$.

Beweis.

- „ $\Longrightarrow$ ": Kontraposition. Sei $a = b$. Dann ist $f(-1) = -1 + a - a + 1 = 0$, also $(X+1) \mid f$ in $\mathbb{Q}[X]$. Es ex. also ein $g \in \mathbb{Q}[X]$, s.d. $f = g \cdot (X+1)$, wegen $\deg(X+1) = 1$ und $f \neq 0$ folgt $\deg(g) = 2$, also $g \notin \mathbb{Q}[X]^\times$. Also f reduzibel in $\mathbb{Q}[X]$. Da $f \notin \mathbb{Z}$ und f primitiv, folgt mit Gauß, dass f auch reduzibel in $\mathbb{Z}[X]$ ist.

  Sei nun $a + b = -2$. Dann ist $f(1) = 1 - 2 - b + b + 1 = 0$. Also $(X-1) \mid f$. Mit analoger Argumentation von oben, ist also f reduzibel in $\mathbb{Z}[X]$.

- „ $\Longleftarrow$ ": Sei nun $a \neq b$ und $a + b \neq -2$. Ang.: f reduzibel in $\mathbb{Z}[X]$. Dann ist f reduzibel in $\mathbb{Q}[X]$ und einer der nichttrivialen Faktoren hat Grad 1, also ex. $\alpha \in \mathbb{Q}$, s.d. $(X - \alpha) \mid f$. Damit folgt $f(\alpha) = 0$. Da f normiert folgt mit (b), dass $\alpha \in \mathbb{Z}$ und $\alpha \mid a_0 = 1$, also $\alpha \in \mathbb{Z}^\times = \{\pm 1\}$. Aber

$$\begin{aligned} f(1) &= 1 + a + b + 1 \overset{a+b\neq -2}{\neq} 0 \\ f(-1) &= -1 + a - b + 1 = a - b \overset{a\neq b}{\neq} 0. \end{aligned}$$

  Also $f(\alpha) \neq 0$ ↯.

□

Aufgabe 4. (a) Beh.: Für $f \in K[X]$ ex. ein solches $a \in R$ und $I(f)$ ist unabhängig von der Wahl von a.

Beweis. Existenz: Sei $f \in K[X]$ und $(p_i)_{i\in I}$ ein Vertretersystem der Primelemente von R. Dann wähle

$$a \coloneqq \prod_{i\in I} p_i^{-\min(v_i(f),0)}.$$

Damit ist $v_i(a) \geq 0\ \forall i \in I$, also $a \in R$. Sei nun $i \in I$ beliebig. Dann ist nach Gauß, da R faktoriell

$$v_i(af) = v_i(a) + v_i(f) = -\min(v_i(f),0) + v_i(f) = \begin{cases} -v_i(f) + v_i(f) = 0 & v_i(f) < 0 \\ v_i(f) \geq 0 & v_i(f) \geq 0 \end{cases}.$$

Also $af \in R[X]$.

Wohldefiniertheit: Seien $a, a' \in R$ mit $af, a'f \in R[X]$. Dann ist für $\epsilon_a, \epsilon_{a'} \in R^\times$:

$$\begin{aligned} I_a(f) &= a^{-1} I(af) \\ &= \epsilon_a \prod_{i\in I} p_i^{-v_i(a)} \prod_{i\in I} p_i^{v_i(af)} \\ &= \epsilon_a \prod_{i\in I} p_i^{v_i(af)-v_i(a)} \\ &\overset{\text{Gauß}}{=} \epsilon_a \prod_{i\in I} p_i^{v_i(f)} \\ &\overset{\wedge}{=} \epsilon'_a \prod_{i\in I} p_i^{v_i(a')+v_i(f)-v_i(a')} \\ &\overset{\text{Gauß}}{=} \epsilon_{a'} \prod_{i\in I} p_i^{-v_i(a')} \prod_{i\in I} p_i^{v_i(af)} \\ &= a'^{-1} I(a'f) \\ &= I_{a'}(f). \end{aligned}$$

□

Für $f = \frac{3}{7}X^2 + X - 5 \in \mathbb{Q}[X]$

$$I(f) = \frac{1}{7} I(7f) = \frac{1}{7} I(3X^2 + 7X - 35) = \frac{1}{7}.$$

(b) Beh.: Für $f, g \in K[X]$ gilt $I(fg) = I(f)I(g)$.

Beweis. Seien $f, g \in K[X]$. Dann ex. mit (b) $a, b \in R$ mit $af, ag \in R[X]$. Dann ist

$$I(fg) = b^{-1}a^{-1} I(abfg) = a^{-1} I(af) b^{-1} I(bg) \iff I(abfg) = I(ab)I(bg).$$

Es genügt also die Behauptung für $f, g \in R[X]$ zu zeigen. Dafür gilt mit $(p_i)_{i\in I}$ Vertretersystem der Primelemente in R:

$$I(fg) = \prod_{i\in I} p_i^{v_i}(fg) \overset{\text{Gauß}}{=} \prod_{i\in I} p_i^{v_i(f)+v_i(g)} = \prod_{i\in I} p_i^{v_i(f)} \prod_{i\in I} p_i^{v_i(g)} = I(f)I(g).$$

□

(c) Sei $r \in R$, $f \in R[X]$ und $h(x) \coloneqq f(X + r) \in R[X]$. Beh.: $I(h) = I(f)$.

Beweis. Falls $\deg(f) = 0$, folgt $f = h$ und damit die Behauptung. Sei also $\deg(f) \geq 1$. Dann sei $a = I(f)$. Dann existiert ein $\tilde{f}$ primitiv, s.d. $f = a\tilde{f}$. Dann ist

$$I(h) = I(f(X + r)) = I(a\tilde{f}(X + r)) \overset{\text{(b)}}{=} aI(\tilde{f}(X + r)) = I(f)I(\tilde{f}(X + r)).$$

Es genügt also zu zeigen, dass $\tilde{f}(X + r)$ primitiv, denn dann ist $I(\tilde{f}(X + r)) = 1$ und damit $I(h) = I(f)$.

Z.z.: $\tilde{f}(X + r)$ primitiv. Sei dazu $p \in R$ Primelement beliebig. Es sei $\deg(h) = \deg(f) =: n \in \mathbb{N}$ und $\tilde{f} = a_n X^n + \ldots + a_0$ und $h = \tilde{a}_n X^n + \ldots + \tilde{a}_0$ mit $\tilde{a}_j, a_j \in R$ für $j \in \mathbb{N}_0$, $j \leq n$. Es ist $a_n = \tilde{a}_n \neq 0$. Falls $v_p(a_n) = v_p(\tilde{a}_n) = 0$, dann fertig. Falls $v_p(a_n) = v_p(\tilde{a}_n) > 0$, dann ex. ein $k \in \mathbb{N}$, s.d. $\forall j \in \mathbb{N}$ mit $k < j \leq n$: $p \mid a_j$ und $p \nmid k$, da $\tilde{f}$ primitiv. Dann betrachte

$$\tilde{a}_k = a_k + \sum_{j=k+1}^{n} \alpha_j a_j \qquad \alpha_j \in R.$$

Da $p \mid a_j$ für $k+1 \leq j \leq n$ folgt $p \mid \sum_{j=k+1}^{n} \alpha_j a_j$ und $p \nmid a_k$, also $p \nmid \tilde{a}_k$. Also folgt $v_p(f(X+r)) = v_p(h) = 0$. Da p beliebig, folgt $\tilde{f}(X + r) = h(X + r)$ primitiv. □

Aufgabe 5. (a) Beh.: $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Beweis. Es ist $z \in Z[i]^\times \iff N(z) = 1$. Offensichtlich ist $N(1) = N(-1) = N(i) = N(-i) = 1$, außerdem folgt aus $N(z) = 1$ mit $z = a + ib$ für $a, b \in \mathbb{Z}$: $a^2 + b^2 = 1$, also $a = 0$ oder $b = 0$. Falls $a = 0 \implies b \in \{\pm 1\}$, analog für $b = 0$. Also insgesamt $z \in \{\pm 1, \pm i\}$. □

(b) Sei $p \in \mathbb{Z}$ Primzahl mit $p = 4n + 1$ mit $n \in \mathbb{N}$. Beh.: $p \mid (2n)!^2 + 1$.

Beweis. Nach dem Satz von Wilson gilt

$$(p-1)! \equiv -1 \pmod{p}$$

Durch Umsortierung folgt mit $p = 4n + 1$

$$1(p-1)2(p-2) \cdot \ldots \cdot 2n(p-2n) \equiv -1 \pmod{p}$$

Da $p - k \equiv -k \pmod{p}$ $\forall k \leq p$, folgt

$$1(-1)2(-2) \cdot \ldots \cdot 2n(-2n) = (-1)^{2n}(2n)!^2 \equiv -1 \pmod{p}$$

Damit folgt

$$(2n)!^2 \equiv -1 \pmod{p}$$

Also ist

$$(2n)!^2 + 1 \equiv 0 \pmod{p}.$$

Also $p \mid ((2n)!^2 + 1)$. □

Beh.: $p \nmid ((2n)! \pm i)$.

Beweis. Ang.: $p \mid ((2n)! \pm i)$. Dann ex. $k \in \mathbb{Z}[i]$ mit $(2n)! \pm i = pk$ und $k = a + ib$ mit $a, b \in \mathbb{Z}$. Dann ist

$$\begin{aligned}(2n)! \pm i &= (4n+1)(a+ib) \\ &= (4n+1)a + i(4n+1)b.\end{aligned}$$

Also folgt $\pm 1 = b\underbrace{(4n+1)}_{>1}$, aber $b \in \mathbb{Z}$ ↯. □

(c) Sei $p \in Z[i]$ Primelement mit $\pi \mid p$ in $\mathbb{Z}[i]$. Beh.: $N(\pi) = p$ und $p = a^2 + b^2$ für $a, b \in \mathbb{Z}$.

Beweis. Da $\pi \mid p$ ex. ein $k \in \mathbb{Z}[i]$ mit $p = \pi k$. Es ist $k \notin \mathbb{Z}[i]^\times$, denn ang. $k \in \mathbb{Z}[i]^\times \implies \pi \hat{=} p$, also p Primelement in $\mathbb{Z}[i]$ ↯ zu (b).

Es ist weiter $p^2 = N(p) = N(\pi)N(k)$. Da $\mathbb{Z}$ faktoriell, p Primzahl in $\mathbb{Z}$, $p^2 \neq 0$ und $\pi, k \notin \mathbb{Z}[i]^\times$ folgt $N(\pi), N(k) \neq 1$ und damit $N(\pi) = N(k) = p$, also $N(\pi) = p$ und damit $p = a^2 + b^2$ für $a, b \in \mathbb{Z}$. □