Aufgabe 1

(a) Es gilt $X^2 - 4 = (X-2)(X+2)$. Da $\mathbb{Q}[X]$ ein faktorieller Ring ist, gibt es eine eindeutige Zerlegung in Primfaktoren. Wäre also $\mathrm{ggT}(f,g) \neq 1$, so müsste $X^3 - 3$ ein Vielfaches von einem der beiden Faktoren sein. Wegen $2^3 - 3 \neq 0$ und $-2^3 - 3 \neq 0$, ist dies aber nicht der Fall. Also ist $\mathrm{ggT}(f,g) = 1$ in $\mathbb{Q}[X]$.

(b) Es gilt $X^2-4 = (X-2)(X+2)$ und $X^3-3 = (X-2)(X^2+2X+4)$. Wegen $(-2)^2+2(-2)+4 = 4 \neq 0$ ist (X^2+2X+4) kein Vielfaches von $(X+2)$, da sonst -2 eine Nullstelle sein müsste. Da $\mathbb{F}_5[X]$ ein faktorieller Ring ist, gibt es eine eindeutige Zerlegung in Primfaktoren. Daher ist $\mathrm{ggT}(f,g) = X-2$ in $\mathbb{F}_5[X]$.

(c) Sei M die Menge aller irreduziblen, normierten Polynome. Angenommen, M ist endlich. Betrachte nun

$$p = \left(\prod_{f \in M} f\right) + 1.$$

Nach Vl gilt $\deg p = \sum_{f\in M} \deg f > \max_{f \in M} \deg f$. Also ist $p \notin M$. Allerdings ist p als Produkt von normierten Polynomen wieder normiert. Daher muss p eine Zerlegung in irreduzible Polynome besitzen. Sei also $p = h \cdot g$ mit $g \in M$. Sei dann $\pi\colon K[X] \to K[X]/(g)$ die kanonische Projektion. Es gilt zunächst $\pi(q) = \pi(h \cdot g) = \pi(h) \cdot \pi(g) = 0$. Allerdings gilt auch

$$\pi\left(\prod_{f\in M} f + 1\right) = \pi\left(\prod_{f\in M} f\right) + \pi(1) = \pi(g) \cdot \pi\left(\prod_{g \neq f \in M} f\right) + \pi(1) = 0 + 1 = 1 \neq 0$$

Das ist ein Widerspruch. Also kann M nicht endlich sein.

(d) Seien $h, h' \in \overline{g}$. Da $K[X]$ euklidisch ist, existieren $q, q', \tilde{g}, \tilde{g}' \in K[X]$ mit $\deg \tilde{g}, \tilde{g}' < \deg f$ und $h = q \cdot f + \tilde{g}$, $h' = q' \cdot f + \tilde{g}'$. Es gilt $0 = \overline{h - h'} = \overline{q \cdot f + \tilde{g} - q' \cdot f - \tilde{g}'} = \overline{q}\overline{f} + \overline{\tilde{g}} - \overline{q'}\overline{f} - \overline{\tilde{g}'} = \overline{\tilde{g} - \tilde{g}'}$. Daraus folgt $\tilde{g} - \tilde{g}' = c \cdot f$ mit $c \in K[X]$. Wegen $\deg \tilde{g}, \deg \tilde{g}' < \deg f \implies \deg(\tilde{g} - \tilde{g}') < \deg f$ und $\deg(cf) = \deg c + \deg f$ muss $\deg c < 0 \Leftrightarrow c = 0$ gelten. Also gilt $\tilde{g} = \tilde{g}' =: g$. Also besitzt jedes Polynom $h \in \overline{g}$ eine eindeutige Darstellung $h = q \cdot f + g$ mit $\deg g < \deg f$. Es gibt also eine injektive Abbildung $\varphi\colon L \to M := \{g \in K \mid \deg g < \deg f\}$. Da durch $\overline{g}$ mit $g \in M$ aber auch eine Äquivalenzklasse gegeben ist, deren eindeutiger Repräsentant genau g sein muss, ist φ sogar eine Bijektion. Da die Polynome $\underline{m} = (1, X, \ldots, X^{\deg f - 1})$ über K linear unabhängig sind und jedes Polynom in M per Definition in $\mathrm{Lin}(\underline{m})$ liegt, ist $\underline{m}$ eine Basis von M, Es gilt also $\dim L = \dim M = \#\underline{m} = \deg f$. Sei $f(X) = a_n X^n + \ldots a_1 X + a_0 \in K[X]$. Dann gilt in $L[X]$

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

Aufgabe 2

(a) Sei $\varphi\colon \mathbb{Z}[X] \to \mathbb{Z}/3\mathbb{Z}[X]$ die kanonische Projektion. Dann gilt $\varphi(f) = X^3 + 2X^2 - 2$. Dieses Polynom ist nach dem Eisensteinkriterium mit $p = 2$ irreduzibel. Nach dem Satz von Gauss ist somit auch $f \in \mathbb{Q}[X]$ irreduzibel.

(b) Sei $f(X) = X^6 + X^3 + 1$. Dann gilt

$$f(X+1) = (X+1)^6 + (X+1)^3 + 1 = X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3$$

Dieses Polynom ist nach dem Eisensteinkriterium mit $p = 3$ irreduzibel. Somit ist auch $f(X)$ irreduzibel. Nach dem Satz von Gauss ist $f(X)$ also auch als Element von $\mathbb{Q}[X]$ irreduzibel.

(c) Wir können $f(X,Y) \in X^7 + 2X^5Y + 3XY^3 + 4Y^3 + 5XY + 6X \in \mathbb{C}[X,Y]$ auch auffassen als Elemente von $\mathbb{C}[X][Y]$. Dann gilt $f(Y) = Y^3(4+3X) + Y(2X^5 + 5X) + X^7 + 6X$. Nach dem Eisensteinkriterium mit $p = X$ (X ist ein Primelement in $\mathbb{C}[X]$) ist f irreduzibel.

Aufgabe 3

(a) Sei $(p_i)_{i\in I}$ ein Vertretersystem von Primelementen in R. Dann gilt

$$a = \prod_{i\in I} p_i^{v_{p_i}(a)}, \qquad b \cdot c = \prod_{i\in I} p_i^{v_{p_i}(b)+v_{p_i}(c)}$$

Gilt $a|x$, so existiert ein $d \in R$ mit $ad = x$. Daher gilt

$$a|bc \qquad \Leftrightarrow \qquad v_{p_i}(a) \leq v_{p_i}(a) + v_{p_i}(d) = v_{p_i}(x) \quad \forall i \in I.$$

Wir wissen also wegen $a|bc$ sofort

$$v_{p_i}(a) \leq v_{p_i}(b) + v_{p_i}(c) \quad \forall i \in I.$$

Ist $\mathrm{ggT}(a,b) = 1$, so gilt $\forall i \in I$

$$\min(v_{p_i}(a), v_{p_i}(b)) = 0.$$

Gälte diese Identität nicht für ein beliebiges $i \in I$, so wäre p_i ein Teiler von a und von b und somit $p_i|\,\mathrm{ggT}(a,b)$. Wir wählen also ein $i \in I$ und unterscheiden zwei Fälle

(1.) $v_{p_i}(a) = 0$. Dann gilt offensichtlich $v_{p_i}(a) \leq v_{p_i}(c)$.

(2.) $v_{p_i}(b) = 0$. Aus $v_{p_i}(a) \leq v_{p_i}(b) + v_{p_i}(c)$ folgt dann $v_{p_i}(a) \leq 0 + v_{p_i}(c) = v_{p_i}(c)$.

Insgesamt gilt also

$$v_{p_i}(a) \leq v_{p_i}(c) \quad \forall i \in I.$$

Das ist äquivalent zu $a|c$.

(b) Ist $f(\alpha) = 0$, so besitzt f die Zerlegung $f(x) = \underbrace{(x-\alpha)}_{=:g} \cdot \underbrace{(X^{n-1} + b_{n-2}X^{n-2} + \cdots + \beta)}_{=:h}$. Da f, g und h normiert sind folgt aus $f \in R[X]$ nach VL $g, h \in R[X]$. Insbesondere gilt also $\alpha, \beta \in R$ und, wie man aus der Produktdarstellung von f leicht sieht, $\alpha \cdot \beta = a_0$. Daher gilt $\alpha|a_0$ in R.

(c) Hier können wir sofort Aufgabe b anwenden. Ist $f := X^3 + aX^2 + bX + 1$ reduzibel, so besitzt es eine Produktdarstellung, wobei mindestens einer der Faktoren Grad 1 besitzen, d.h. von der Form $(X - \alpha)$ sein muss. Also muss f eine Nullstelle besitzen. Diese muss nach b aber ein Teiler von 1 in $\mathbb{Z}$ sein, also $\alpha = \pm 1$. Es gilt aber

$$0 = f(1) = 1 + a + b + 1 \qquad \Leftrightarrow \qquad a + b = -2$$

und

$$0 = f(-1) = -1 + a - b + 1 \qquad \Leftrightarrow \qquad a - b = 0 \Leftrightarrow a = b.$$

Daher ist f genau dann irreduzibel, wenn $a + b = -2$ oder $a = b$ gilt.

Aufgabe 4

Sei $(p_i)_{i\in I}$ ein Vertretersystem von Primelementen in R.

(a) Sei $f = a_nX^n + \dots a_1X^1 + a_0$ Wähle $a = \prod_{i\in I} p_i^{-\min(v_{p_i}(f),0)}$. Dann gilt nämlich

$$v_{p_i}(a\cdot f) = v_{p_i}(a) + v_{p_i}(f) = -\min(v_{p_i}(f), 0) + v_{p_i}(f).$$

Ist nun für ein $i \in I$ $v_{p_i}(f) < 0$, so gilt $v_{p_i}(a\cdot f) = -\min(v_{p_i}(f), 0)+v_{p_i}(f) = -v_{p_i}(f)+v_{p_i}(f) = 0$. Gilt $v_{p_i}(f) \geq 0$, so ändert sich nichts. Es existiert also ein solches a. Für beliebiges a mit $a\cdot f \in R$ gilt

$$\begin{aligned} I(f) &= a^{-1}\cdot \mathrm{ggT}(a\cdot a_0, \dots, a\cdot a_n) \\ &= \prod_{i\in I} p_i^{-v_{p_i}(a)} \cdot \prod_{i\in I} p_i^{\min(v_{p_i}(a\cdot a_0),\dots,v_{p_i}(a\cdot a_n))} \\ &= \prod_{i\in I} p_i^{-v_{p_i}(a)} \cdot \prod_{i\in I} p_i^{v_{p_i}(a)+\min(v_{p_i}(a_0),\dots,v_{p_i}(a_n))} \\ &= \prod_{i\in I} p_i^{-v_{p_i}(a)} \cdot \prod_{i\in I} p_i^{v_{p_i}(a)+v_{p_i}(f)} \\ &= \prod_{i\in I} p_i^{v_{p_i}(f)} \end{aligned}$$

Damit ist $I(f)$ unabhängig von der Wahl von a. Für $f = \frac{3}{7}X^3 + X - 5$ gilt

$$I(f) = \frac{1}{7}\,\mathrm{ggT}(3, 7, -35) = \frac{1}{7}.$$

(b) Es gilt

$$\begin{aligned} I(f\cdot g) &\overset{\text{Teilaufgabe (a)}}{=} \prod_{i\in I} p_i^{v_{p_i}(f\cdot g)} \\ &\overset{\text{Vorlesung}}{=} \prod_{i\in I} p_i^{v_{p_i}(f)+v_{p_i}(g)} \\ &= \prod_{i\in I} p_i^{v_{p_i}(f)} \cdot \prod_{i\in I} p_i^{v_{p_i}(g)} \\ &\overset{\text{Teilaufgabe (a)}}{=} I(f)\cdot I(g) \end{aligned}$$

(c) Es gilt allgemein:

$$d|a_0 \wedge d|a_1 \Leftrightarrow d|a_1 + \lambda a_0.$$

Daraus folgt

$$\mathrm{ggT}(a_0, a_1) = \mathrm{ggT}(a_0, a_0 + \lambda a_1).$$

Per Induktion folgt daraus

$$\mathrm{ggT}(a_n, a_{n-1} + \lambda a_n, \dots, a_0 + \sum_{i=1}^{n} \lambda_i a_i) = \mathrm{ggT}(a_n, \dots, a_0).$$

Sei also $f(X) = \sum_{i=0}^{n} a_i X^i$. Dann gilt

$$h(X) = \sum_{i=0}^{n} a_i (X+r)^i = \sum_{i=0}^{n} a_i \sum_{j=0}^{i} \binom{i}{j} r^{i-j} X^j$$

X^j taucht Für den Vorfaktor b_j von X^j in h gilt nun $b_j = \sum_{i=j}^{n} a_i \binom{i}{j} r^{i-j} = a_j + \sum_{i=j+1}^{n} a_i \binom{i}{j} r^{i-j}$. Es gilt daher

$$I(h) = \operatorname{ggT}(b_n, \dots, b_0) = \operatorname{ggT}\left(a_n, \dots, a_0 + \sum_{i=1}^{n} a_i \binom{i}{j} r^{i-j}\right) = \operatorname{ggT}(a_n, \dots, a_0) = I(f).$$

Bonusaufgabe 5

(a) Wir zeigen u Einheit $\implies N(u) = 1 \implies u \in \{\pm 1, pmi\} \implies u$ Einheit und damit die Äquivalenz dieser Aussagen. Sei also u eine Einheit. Dann $\exists v$ mit $u \cdot v = 1 \implies N(u \cdot v) = 1 = N(u) \cdot N(v)$. Wegen $N(x) > 0 \forall x \in \mathbb{Z}[i]$ muss $N(u) = N(v) = 1$ gelten. Sei nun $N(u) = 1$. u besitzt eine Darstellung durch $u = a + b \cdot i$. Wegen $N(u) = 1$ muss also $a^2 + b^2 = 1$ gelten. Also ist $u \in \{\pm 1, \pm i\}$. Da $\{\pm 1, \pm i\}$ offensichtlich Einheiten sind, folgt die Behauptung.

(b) Behauptung: $(4n+1) | [(2n)!^2 - (4n)!]$.

Beweis. Es gilt $(2n)!^2 - (4n)! = (2n)! \cdot \left((2n)! - \prod_{i=2n+1}^{4n} i\right)$. Da $(4n+1) \not| (2n)!$, konzentrieren wir uns auf den zweiten Faktor.

$$(2n)! - \prod_{i=2n+1}^{4n} i = (2n)! - \prod_{i=1}^{2n} ((4n+1) - i)$$

Wenden wir das Distributivgesetz auf dieses Produkt an, so erhalten wir für ein irrelevantes α

$$\begin{aligned} &= (2n)! - \alpha(4n+1) - \prod_{i=1}^{2n}(-i) \\ &= (2n)! - (-1)^{2n}(2n)! - \alpha(4n+1) \\ &= -\alpha(4n+1) \end{aligned}$$

Daraus folgt bereits die Behauptung. □

Da $4n+1$ eine Primzahl ist, gilt nach dem Satz von Wilson $(4n)! \equiv -1 \mod (4n+1) \Leftrightarrow (4n+1) | (4n!) + 1$. Es gilt $(2n)!^2 + 1 = ((2n)!^2 + 1) - (4n)! + 1) + (4n)! + 1 = [(2n)!^2 - (4n)!] + (4n)! + 1$ und wegen $c | [(2n)!^2 - (4n)!], c | (4n)! + 1$ folgt daraus $c | (2n)!^2 + 1$.

Angenommen, $\exists c + di \in \mathbb{Z}[i]$ mit $(c + di) \cdot (4n+1) = (2n)! \pm i$. Dann folgt aus separater Betrachtung von Real- und Imaginärteil $d \cdot (4n+1) = \pm 1$ mit $d, n \in \mathbb{Z}$. Das ist offensichtlich ein Widerspruch. Daher kann p kein Primelement in $Z[i]$ sein.

(c) Wegen $\pi | p$ gilt auch $N(\pi) | N(p) = p^2$. Da p eine Primzahl ist und π als Primelement keine Einheit sein darf, muss also entweder $N(\pi) = p$ oder $N(\pi) = p^2$ gelten. Angenommen, $N(\pi) = p^2 = N(p)$. Wegen $\pi | p$ existiert ein $c \in \mathbb{Z}[i]$ mit $p = c \cdot \pi$. Daraus folgt $N(p) = N(c) \cdot N(\pi) = N(c) \cdot N(p) \implies N(c) = 1$. Wegen Teilaufgabe a muss also c eine Einheit sein, es folgt also $\pi \hat{=} p$. Dann folgt aber aus Teilaufgabe b völlig analog, dass π kein Primelement sein kann. Die einzige verbleibende Möglichkeit ist $N(\pi) = p$. Wegen $\pi | p | (2n)!^2 + 1$ und π prim, muss π auch eine der beiden Zahlen $(2n)! \pm i$ teilen. Angenommen, $\Im \pi = 0$. Dann folgt die Gleichung $\pi \cdot (a + bi) = (2n)! \pm i$ und, bei separater Betrachtung von Real- und Imaginärteil erhalten wir $\pi \cdot b = \pm 1, \pi, b \in \mathbb{Z}$. Wegen $\pi \neq 1$ ist das ein Widerspruch. Also ist $\Im \pi \neq 0$. Angenommen, $\Re \pi = 0$. Dann folgt die Gleichung $\pi \cdot (a + bi) = (2n)! \pm i$ und, bei separater Betrachtung von Real- und Imaginärteil erhalten wir $\pi \cdot a = \pm 1, \pi, a \in \mathbb{Z}$. Wegen $\pi \neq 1$ ist auch das ein Widerspruch. Daher ist $\pi = a + bi$ mit $a, b \in \mathbb{Z} \setminus \{0\}$. Insbesondere ist daher $p = N(\pi) = a^2 + b^2$ mit $a, b \neq 0$. Damit ist der Zwei-Quadrate-Satz bewiesen.