Blatt 2

(1) a) $z = a + b\sqrt{-5}, \quad w = c + d\sqrt{-5}$

$\Rightarrow zw = ac - 5bd + (ad + bc)\sqrt{-5}$

$\Rightarrow N(zw) = (ac - 5bd)^2 + 5(ad + bc)^2$

$= a^2c^2 + 25b^2d^2 - 10abcd + 5a^2d^2 + 5b^2c^2 + 10abcd$

$= a^2c^2 + 25b^2d^2 + 5a^2d^2 + 5b^2c^2$

$= (a^2 + 5b^2)(c^2 + 5d^2) = N(z)N(w)$

b) $\Leftarrow$: $z = a + b\sqrt{-5}, \ a, b \in \mathbb{Z}, \ N(z) = 1$

$\Rightarrow a^2 + 5b^2 = 1 \Rightarrow a = \pm 1, \ b = 0$

$\Rightarrow z = \pm 1 \Rightarrow z \in \mathbb{Z}[\sqrt{-5}]^*$

$\Rightarrow$: $z \in \mathbb{Z}[\sqrt{-5}]^* \Rightarrow \exists\, w \in \mathbb{Z}[\sqrt{-5}] : zw = 1$

$\Rightarrow N(zw) = N(1) = 1$

$\underset{a)}{\Rightarrow} N(z)N(w) = 1 \Rightarrow N(z) = 1$

Da $N(z) = 1 \Leftrightarrow z = \pm 1$ folgt $\mathbb{Z}[\sqrt{-5}]^* = \{\pm 1\}$

c) $z = uv \Rightarrow N(z) = N(u)N(v)$

Falls z nicht irreduzibel, so gibt es eine Zerlegung $z = uv$ mit $u, v \notin \mathbb{Z}[\sqrt{-5}]^*$ also $N(u) \neq 1$, $N(v) \neq 1$

Dann sind $N(u)$, $N(v)$ echte Teiler von $N(z)$

Betrachte nun $z = 2, 3, 1 \pm \sqrt{-5}$

Es gilt $N(2) = 4$, $N(3) = 9$, $N(1 \pm \sqrt{-5}) = 6$

Die echten Teiler sind 2 oder 3

Es gibt aber keine Elemente in $\mathbb{Z}[\sqrt{-5}]$ mit $N(u) = 2$ oder $N(u) = 3$, da die Gleichungen

$$a^2 + 5b^2 = 2 \quad , \quad a^2 + 5b^2 = 3$$

jeweils keine Lösung haben mit $a, b \in \mathbb{Z}$

Somit sind $2, 3, 1 \pm \sqrt{-5}$ irreduzibel in $\mathbb{Z}[\sqrt{-5}]$

Falls $z \mid w$ in $\mathbb{Z}[\sqrt{-5}]$ so folgt $w = zu$ und nach a): $N(w) = N(z)N(u)$

also $N(z) \mid N(w)$ falls $z \mid w$

Daraus folgt: $2, 3$ teilen nicht $1 \pm \sqrt{-5}$

und $1 \pm \sqrt{-5}$ teilen nicht $2, 3$

Wegen $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$

können daher $2, 3, 1 \pm \sqrt{-5}$ allesamt keine Primelemente sein.

d) Da es in $\mathbb{Z}[\sqrt{-5}]$ irreduzible Elemente gibt, die keine Primelemente sind, ist $\mathbb{Z}[\sqrt{-5}]$ nach 5.1.15 nicht faktoriell

(Konkret hat 6 in $\mathbb{Z}[\sqrt{-5}]$ keine Primfaktorzerlegung)

② a) <u>Ann:</u> $I = (h)_{\mathbb{Z}[t]}$ sei ein Hauptideal

$2 \in I \Rightarrow \exists\, g_1 \in \mathbb{Z}[t]$ mit $2 = g_1 \cdot h$

$\Rightarrow \operatorname{grad}(h) = 0$ und da $1 \notin I$ bleibt nur $h = \pm 2$ übrig

$t \in I \Rightarrow \exists\, g_2 \in \mathbb{Z}[t]$ mit

$$t = g_2 h = \pm 2 g_2$$

$\Rightarrow$ t hat nur gerade Koeffizienten

<u>Wid.</u>

$\Rightarrow$ I kein Hauptideal

b) $$t^6 - 1 = (t^3 - 1)(t^3 + 1)$$

$$= (t-1)(t^2 + t + 1)(t+1)(t^2 - t + 1)$$

Die Polynome $t-1$, $t+1$ sind offensichtlich irreduzibel in $\mathbb{Z}[t]$

$t^2 + t + 1$, $t^2 - t + 1$ sind irreduzibel in $\mathbb{Z}[t]$, da sie Polynome zweiten Grades sind und in $\mathbb{Z}$ keine Nullstelle haben

③ a)

$$531 = 5 \cdot 93 + 66$$
$$93 = 66 + 27$$
$$66 = 2 \cdot 27 + 12$$
$$27 = 2 \cdot 12 + 3$$
$$12 = 4 \cdot 3$$

$\Rightarrow 3 = ggT(531, 93)$

Zurückrechnen liefert

$$3 = 40 \cdot 93 - 7 \cdot 531$$

b)

$$247 = 221 + 26$$
$$221 = 8 \cdot 26 + 13$$
$$26 = 2 \cdot 13$$

$\Rightarrow 13 = ggT(247, 221)$ und

$$13 = -8 \cdot 247 + 9 \cdot 221$$

c)

$$t^3 + 4t^2 + 5t + 2 = (t^3 - 3t + 2) + 4t^2 + 8t$$
$$t^3 - 3t + 2 = (4t^2 + 8t)\left(\tfrac{1}{4}t - \tfrac{1}{2}\right) + t + 2$$
$$4t^2 + 4t = 4t(t+2)$$

$\Rightarrow$ Der ggT ist $t+2$ und es gilt

$$t + 2 = \left(\tfrac{1}{4}t + \tfrac{1}{2}\right)(t^3 - 3t + 2) - \left(\tfrac{1}{4}t - \tfrac{1}{2}\right)(t^3 + 4t^2 + 5t + 2)$$

d) $t^6+1 = t(t^5+2t^3+t^2+t+1)+3t^4+4t^3+4t^2+4t+1$

$$t^5+2t^3+t^2+t+1 = (2t+4)(3t^4+4t^3+4t^2+4t+1) + 3t^3+2t^2+3t+2$$

$$3t^4+4t^3+4t^2+4t+1 = (t+4)(3t^3+2t^2+3t+2)+3t^2+3$$

$$3t^3+2t^2+3t+2 = (t+4)(3t^2+3)$$

$\Rightarrow$ ggT ist $3t^2+3$

Mit $P := t^6+1$, $Q := t^5+2t^3+t^2+t+1$

gilt nach Zurückrechnen:

$$3t^2+3 = (2t^2+2t+2)P - (2t^3+2t^2+3t+4)Q$$

④ a) Sei $\alpha \in K[t]/I$, also
$\alpha = f + I$ mit $f \in K[t]$
Division mit Rest:
$$f = \tilde{q}\, p + q \quad \text{mit } q, \tilde{q} \in K[t]$$
$$\operatorname{grad}(q) < \operatorname{grad}(p)$$

$\Rightarrow f + I = q + I$, da $f - q = \tilde{q} p \in I$

$\Rightarrow \alpha \in \{ q + I \mid \operatorname{grad}(q) < \operatorname{grad}(p) \}$

b) $\beta_i := t^i + I$, $i = 0, \dots, n-1$ $(t^0 = 1)$

$\beta_0, \dots, \beta_{n-1}$ sind linear unabhängig:

Sei $\sum_{i=0}^{n-1} b_i \beta_i = 0$ mit $b_i \in K$

$\Rightarrow \sum_{i=0}^{n-1} b_i t^i = g p$ mit $g \in K[t]$

$\underset{\operatorname{grad}(p) = n}{\Longrightarrow} \sum_{i=0}^{n-1} b_i t^i = 0$

$\Rightarrow b_i = 0 \quad (i = 0, \dots, n-1)$

$\beta_0, \dots, \beta_{n-1}$ sind ein ES:

Sei $\alpha \in K[t]/I$

Nach a) gilt $\alpha = q + I$ mit $\operatorname{grad}(q) < n$

$\Rightarrow q = \sum_{i=0}^{n-1} b_i t^i$ mit $b_i \in K$

$\Rightarrow \alpha = q + I = \sum_{i=0}^{n-1} b_i \beta_i$