Algebra - Blatt 8

A1) (a) Nein. Sei $f \in \mathbb{Z}[X]$ mit $2, X \in (f)$. Dann folgt $2 = f \cdot g$ und $X = f \cdot h$ für geeignete $g, h \in \mathbb{Z}[X]$, d.h. $f \mid 2$ und $f \mid h$. Nach A1(c) folgt $f = \pm 1$, also $(f) = \mathbb{Z}[X]$.

(b) Nein. $2X^2 + 4 = 2 \cdot (X^2 + 2)$ und weder 2 noch $X^2 + 2$ sind Einheiten in $\mathbb{Z}[X]$.

(c) Ja. Die einzigen Teiler von 2 sind ± 1 und ± 2, die einzigen Teiler von X sind ± 1 und $\pm X$.

A2) (a) Sei $f \in \mathbb{C}[X]$. Nach dem Hauptsatz der Algebra ist

$$f = c(X - a_1) \cdot \ldots \cdot (X - a_n)$$

für geeignete $c \in \mathbb{C}$, $a_1, \ldots, a_n \in \mathbb{C}$, $n = \deg(f)$.

Falls $\deg(f) = 0$ oder $f = 0$, so ist f nicht irreduzibel (per Def.).
($\deg(f) = 0 \Rightarrow f$ ist Einheit in $\mathbb{C}[X]$)

Falls $\deg(f) > 1$, so ist $f = \underbrace{c \cdot (X - a_1)}_{\text{keine Einheit in } \mathbb{C}[X]} \cdot \underbrace{(X - a_2) \cdot \ldots \cdot (X - a_n)}_{\text{keine Einheit in } \mathbb{C}[X]}$

also f nicht irreduzibel.

Falls $\deg(f) = 1$, so ist $f = c \cdot (X - a_1)$ irreduzibel:

Seien $g, h \in \mathbb{C}[X]$ mit $f = g \cdot h$. Dann ist $g(a_1) \cdot h(a_1) = f(a_1) = 0$, also $g(a_1) = 0$ oder $h(a_1) = 0$. o.E. $g(a_1) = 0$. Dann ist $g = c'(X - a_1)$, also $h = \frac{c}{c'} \in (\mathbb{C}[X])^*$. $\Rightarrow f$ irreduzibel.

A2)(b) Sei $f \in \mathbb{R}[X]$. Fasse f als Polynom in $\mathbb{C}[X]$ auf und schreibe $f = c\cdot(X-a_1)\cdots(X-a_n)$, $c, a_1, \dots, a_n \in \mathbb{C}$.

Nach dem Hinweis ist $\{a_1, \dots, a_n\} = \{b_1, \dots, b_m, \overline{b_1}, \dots, \overline{b_m}, c_1, \dots, c_\ell\}$ für geeignete $b_1, \dots, b_m \in \mathbb{C}\setminus\mathbb{R}$, $c_1, \dots, c_\ell \in \mathbb{R}$. $(\ell + 2m = n)$

Also
$$f = c\cdot(X-b_1)(X-\overline{b_1})\cdots(X-b_m)(X-\overline{b_m})(X-c_1)\cdots(X-c_\ell)$$

Wenn nun $\deg(f) = n > 2$ ist, so ist $m \geq 2$ oder $\ell \geq 2$ oder ($m = 1$ und $\ell = 1$). (Denn ($m \leq 1$ und $\ell \leq 1$) $\Rightarrow n \leq 3$, und $n = 3$ nur für $m = \ell = 1$.)

1. Fall $m \geq 2$. Dann ist
$$f = \underbrace{c(X-b_1)(X-\overline{b_1})}_{\in \mathbb{R}[X]\setminus(\mathbb{R}[X])^\times \text{ keine Einheit in } \mathbb{R}[X]} \cdot \underbrace{(X-b_2)(X-\overline{b_2})\cdots(X-b_m)(X-\overline{b_m})(X-c_1)\cdots(X-c_\ell)}_{\in \mathbb{R}[X]\setminus(\mathbb{R}[X])^\times}.$$

2. Fall $\ell \geq 2$. Dann ist
$$f = \underbrace{c(X-b_1)\cdots(X-\overline{b_m})(X-c_1)}_{\in \mathbb{R}[X]\setminus\mathbb{R}[X]^\times} \cdot \underbrace{(X-c_2)\cdots(X-c_\ell)}_{\in \mathbb{R}[X]\setminus\mathbb{R}[X]^\times}$$

3. Fall $m = \ell = 1$. Dann ist
$$f = \underbrace{c(X-b_1)(X-\overline{b_1})}_{\in \mathbb{R}[X]\setminus\mathbb{R}[X]^\times} \underbrace{(X-c_1)}_{\in \mathbb{R}[X]\setminus\mathbb{R}[X]^\times}$$

In allen drei Fällen ist f also nicht irreduzibel.

$\Rightarrow$ oder h ist Einheit ($\Leftrightarrow$ Unmöglich!) oder hat Nullstelle

(c) $f = X^3 - 2 \in \mathbb{Q}[X]$ hat keine Nullstelle in $\mathbb{Q}$ und ist daher irreduzibel! $f = gh \Rightarrow \deg(g) + \deg(h) = 3 \Rightarrow g$ oder h hat Grad ≤ 1 $\Uparrow$

A3) $R' = \{ \frac{a}{b} \mid a \in R, b \in S \} \subseteq Quot(R)$

(a) • $(R', +)$ ist abelsche Gruppe: $\frac{a}{b}, \frac{c}{d} \in R'$, dann

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \in R'$$
$\in R$ $\in S$ da S multipl. abg.

und $-\frac{a}{b} = \frac{(-a)}{b} \in R'$ sowie $0 = \frac{0}{b} \in R'$

$\rightsquigarrow$ Da $(Quot(R), +)$ eine ab. Grp. ist und $R' \subseteq Quot(R)$ abgeschlossen bzgl. $+$, ist $(R', +)$ ab. Grp.

• Für $\frac{a}{b}, \frac{c}{d} \in R'$ ist $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d} \in R'$,
$\in R$ $\in S$

Assoziativität und Kommutativität von "$\cdot$" vererbt sich direkt vom $Quot(R) \supseteq R'$; genauso Distributivität.

• $1 = \frac{a}{a} \in R'$ für beliebiges $a \in S$.

(b) Wir zeigen: Sind $\mathfrak{a}_1, \mathfrak{a}_2 \subseteq R'$ Ideale mit $\mathfrak{a}_1 \cap R \subseteq \mathfrak{a}_2 \cap R$, so ist $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$.
(Daraus folgt die Behauptung aus Symmetriegründen.)

Bew: Sei $x \in \mathfrak{a}_1$, etwa $x = \frac{a}{b}$. Dann ist $a = b \cdot x \in \mathfrak{a}_1 \cap R$, also $a \in \mathfrak{a}_2 \cap R \subseteq \mathfrak{a}_2$. Wegen $\frac{1}{b} \in R'$ folgt $x = a \cdot \frac{1}{b} \in \mathfrak{a}_2$.

(c) Sei R ein Hauptidealring und $\mathfrak{a} \subseteq R'$ ein Ideal. Dann ist $\mathfrak{a} \cap R$ ein Ideal von R, also $\mathfrak{a} \cap R = xR$ für geeignetes $x \in R$.

Beh: $\mathfrak{a} = xR'$. (Insbesondere ist $\mathfrak{a}$ ein Hauptideal.)

Bew: Klar ist $x \in \mathfrak{a} \cap R \subseteq \mathfrak{a}$, also $xR' \subseteq \mathfrak{a}$.
Außerdem ist $\mathfrak{a} \cap R = xR \subseteq xR' \cap R$, d.h. nach A3 (b) ist $\mathfrak{a} \subseteq xR'$. Insgesamt $\mathfrak{a} = xR'$.

A4) (a) Wie in A3(a) zeigen wir Abgeschlossenheit unter + und ·, Existenz additiver Inverser und $0, 1 \in R$.
Da $R \subseteq \mathbb{C}$ und $\mathbb{C}$ ein Ring ist (und die Verknüpfungen auf R durch Einschränkung der Verknüpfungen auf $\mathbb{C}$ gegeben sind!) genügt dies.

- Für $r+si, r'+s'i \in R$ (d.h. $r, s, r', s' \in \mathbb{Z}$) ist

$$r+si + r'+s'i = \underbrace{r+r'}_{\in\mathbb{Z}} + \underbrace{(s+s')}_{\in\mathbb{Z}} i \in R,$$

$$-(r+si) = \underbrace{-r}_{\in\mathbb{Z}} + \underbrace{(-s)}_{\in\mathbb{Z}} i \in R \text{ und}$$

$$(r+si)(r'+s'i) = \underbrace{(rr'-ss')}_{\in\mathbb{Z}} + \underbrace{(rs'+r's)}_{\in\mathbb{Z}} i \in R$$

- $0 = 0+0\cdot i$ und $1 = 1+0\cdot i \in R$.

Dass R ein Integritätsbereich ist folgt, da $\mathbb{C}$ einer ist: Ein Nullteiler in R wäre auch Nullteiler in $\mathbb{C}$!

(b) Es ist klar, dass ± 1 und $\pm i$ Einheiten sind, denn $1^2 = (-1)^2 = i\cdot(-i) = 1$
Sei nun $a \in R^\times$ beliebig. Betrachte $b \in R$ mit $a\cdot b = 1$. Es ist
$1 = |ab|^2 = (|a|\cdot|b|)^2 = |a|^2\cdot|b|^2$ für die komplexe Norm $|\cdot|$
(Beachte, dass $a, b \in \mathbb{C}$) Beh.: $|x|^2 \in \mathbb{N}$ für $x \in R$
Bew.: Sei $x = r+si$. $|x|^2 = |r+si|^2 = \sqrt{r^2+s^2}^2 = r^2+s^2 \in \mathbb{N}$.

Also $1 = \underbrace{|a|^2}_{\in\mathbb{N}}\cdot\underbrace{|b|^2}_{\in\mathbb{N}}$ und damit $|a|^2 = 1$.

Wäre nun $a = r+si$ mit $(r,s) \notin \{(\pm 1, 0), (0, \pm 1)\}$, so wäre $|a|^2 = r^2+s^2 > 1$, also $a \notin R^\times$. Es folgt $a \in \{\pm 1, \pm i\}$, d.h. $\{\pm 1, \pm i\} \supseteq R^\times$; insgesamt $R^\times = \{\pm 1, \pm i\}$.

(c) Seien $a, b \in \mathbb{Z}[i] \setminus \{0\}$, etwa $a = a_1 + a_2 i$, $b = b_1 + b_2 i$, mit $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Betrachte $\frac{a}{b} \in \mathbb{C}$, es ist

$$\frac{a}{b} = \frac{a\bar{b}}{b\bar{b}} = \frac{a\bar{b}}{b_1^2+b_2^2} \in \mathbb{Z}[i] \\ \frac{a\bar{b}}{b_1^2+b_2^2} \in \mathbb{N}_{>0} \Big\} \in \mathbb{Q}[i] = \{q_1 + q_2 i \mid q_1, q_2 \in \mathbb{Q}\} \subseteq \mathbb{C}$$

also $\frac{a}{b} = q_1 + q_2 i$ für $q_1, q_2 \in \mathbb{Q}$ geeignet.

Finde (durch Auf-/Abrunden) $c_1, c_2 \in \mathbb{Z}$ mit $|q_1 - c_1| \leq \frac{1}{2}$ und $|q_2 - c_2| \leq \frac{1}{2}$.

Beh: $c := c_1 + c_2 i \in \mathbb{Z}[i]$ und $r := a - bc \in \mathbb{Z}[i]$ erfüllen

$$a = bc + r \text{ und } \begin{cases} r = 0 \text{ oder} \\ \sigma(r) < \sigma(b). \end{cases}$$

Bew: $a = bc + r$ ist klar nach Def. von r.

$c \in \mathbb{Z}[i]$ ist klar nach Wahl von c.

$r \in \mathbb{Z}[i]$ ist klar, da $r = a - bc$ mit $a, b, c \in \mathbb{Z}[i]$.

Bleibt zz: Falls $r \neq 0$, so ist $\sigma(r) < \sigma(b)$. Sei also $r \neq 0$.

Beachte, dass $\sigma(r) = |r|^2 = |a - bc|^2 = |\underbrace{b(q_1+q_2 i)}_{=a} - \underbrace{b(c_1+c_2 i)}_{=bc}|$

$= |b \cdot \underbrace{(q_1+q_2 i - (c_1+c_2)i)}_{=(q_1-c_1)+(q_2-c_2)i}|^2 = |b|^2 \cdot (\underbrace{(q_1-c_1)^2}_{\leq (\frac{1}{2})^2} + \underbrace{(q_2-c_2)^2}_{\leq (\frac{1}{2})^2}) \leq \frac{1}{2}|b|^2 < |b|^2$ (b ≠ 0) $= \sigma(b)$.

Wir habe damit gezeigt, dass R mit δ euklidisch ist, nach Satz 2.5.10 also insbesondere ein Hauptidealring und nach Satz 2.5.12. insbesondere faktoriell.

(d) Es ist $(1+i)(1-i) = 1^2 - i^2 = 1+1 = 2$,
dabei sind $1+i$ und $1-i \notin R^\times$ nach A 4(b).
Also ist 2 nicht irreduzibel in R.