(A.) Sei $\mathbb{Z}[\omega] = \{a+b\omega \mid a,b \in \mathbb{Z}\}$ mit $\omega = \frac{1}{2}(-1+i\sqrt{3})$.

(a) z.z.: $\mathbb{Z}[\omega]$ ist euklidischer Ring mit Norm $N(a+b\omega) = a^2 - ab + b^2$.

- $(a+b\omega) + (c+d\omega) = (a+c) + (b+d)\omega$
- $(a+b\omega)\cdot(c+d\omega) = ac + (ad+bc)\omega + bd\omega^2$, und es gilt $\omega^2 \in \mathbb{Z}[\omega]$:
- $\omega^2 = \frac{1}{4}(1 - 2i\sqrt{3} - 3) = \frac{1}{4}(-2 - 2i\sqrt{3}) = -\frac{1}{2}(1+i\sqrt{3}) = -\frac{1}{2}(-1+i\sqrt{3}) - 1 = -\omega - 1$.
- $\mathbb{Z}[\omega]$ erbt alle Rechengesetze und die Nullteilerfreiheit von $\mathbb{C}$, ist also ein Integritätsbereich.

„Division mit Rest": $\forall z_1, z_2 \in \mathbb{Z}[\omega], z_2 \neq 0 \; \exists q, r \in \mathbb{Z}[\omega]: z_1 = q z_2 + r$ mit $N(r) \leq N(z_2)$.

$$\underbrace{\frac{z_1}{z_2}}_{\in \mathbb{C}} = \underbrace{(a+b\omega)}_{\text{nächstliegende Zahl in } \mathbb{Z}[\omega]} + \underbrace{(s_1 + i s_2)}_{s_1, s_2 \in \mathbb{R}} = \underbrace{(a+b\omega)}_{=:q} + \underbrace{(t_1 + t_2\omega)}_{=:t}.$$

(Wir können jedes $z \in \mathbb{C}$ in die Form $t_1 + \omega t_2$, $t_1, t_2 \in \mathbb{R}$ bringen vermöge des Basiswechsels $x+iy = \binom{x}{y} \mapsto A^{-1}\binom{x}{y} = \begin{pmatrix} 1 & 1/\sqrt{3} \\ 0 & 2/\sqrt{3} \end{pmatrix}\binom{x}{y}$, wobei $A = \begin{pmatrix} 1 & -1/2 \\ 0 & \underbrace{\sqrt{3}/2}_{=\omega} \end{pmatrix}$,

bzw. $x+iy = \left(x + \frac{y}{\sqrt{3}}\right) + \left(\frac{2}{\sqrt{3}}y\right)\omega$.)

Nun gilt $\underbrace{z_1}_{\in \mathbb{Z}[\omega]} = \underbrace{q}_{\in \mathbb{Z}[\omega]} \cdot z_2 + \underbrace{t}_{\in \mathbb{Z}[\omega]} \cdot z_2 \Rightarrow \underbrace{\quad}_{=:r \in \mathbb{Z}[\omega]}$.

Der max. Abstand von einem $z \in \mathbb{C}$ zu $\mathbb{Z}[\omega]$ ist der Abstand des Mittelpunkts eines der von $\mathbb{Z}[\omega]$ aufgespannten Parallelogramme zu dessen Ecken, also $\left\| \frac{1+\omega}{2} \right\|_2 = \left\| \frac{1}{4} + \frac{\sqrt{3}}{4} i \right\|_2 = \sqrt{\frac{1}{4}} = \frac{1}{2}$, d.h. $\|s\|_2 \leq \frac{1}{2}$ und folglich

$$\begin{aligned} N(r) = N(t \cdot z_2) &= N(t)\,N(z_2) = (t_1^2 - t_1 t_2 + t_2^2)\,N(z_2) \\ &= \left[\left(s_1 + \frac{s_2}{\sqrt{3}}\right)^2 - \left(s_1 + \frac{s_2}{\sqrt{3}}\right)\left(\frac{2}{\sqrt{3}} s_2\right) + \left(\frac{2}{\sqrt{3}} s_2\right)^2 \right] N(z_2) \\ &\overset{\text{(MAPLE)}}{=} (s_1^2 + s_2^2)\,N(z_2) \leq \frac{1}{4} N(z_2) < N(z_2). \end{aligned}$$

Dabei haben wir die Multiplikativität der Norm verwendet, die man leicht nachrechnen kann.

(b) Einheiten von $\mathbb{Z}[\omega]$: $a+b\omega$ Einheit $\Rightarrow N(a+b\omega) = 1 \left[\Leftrightarrow (a-b)^2 + ab = 1\right]$.

Falls $a, b > 1$, gilt wegen $(a-b)^2 > 0$ $N(a+b\omega) > 1$; dasselbe passiert, wenn $a > 2$ und $b \neq 0$ oder $b > 2$ und $a \neq 0$. Weiters gilt $a, b = 0 \Rightarrow N(a+b\omega) = 0$. Auch $a > 2 \wedge b = 0$ und $b > 2 \wedge a \neq 0$ ist unmöglich. Alle bisher behandelten Fälle mit umgekehrtem Vorzeichen erweisen sich ebenso als unmöglich, weiters auch $a \geq 1$ und $b \leq -1$, $a \leq -1$ und $b \geq 1$; die verbliebenen Fälle sind also $a = b = 1$, $a = b = -1$, $a = 0 \wedge b = 1$, $a = 1 \wedge b = 0$, $a = 0 \wedge b = -1$, $a = -1 \wedge b = 0$, also ist $\{1+\omega, -\omega-1 = \omega^2, \omega, 1, -\omega, -1\}$ die Menge der möglichen Einheiten. Es verbleibt die Verifikation, dass es sich tatsächlich um Einheiten handelt.

Zum Beispiel gilt $\frac{1}{\omega} = \frac{\overline{\omega}}{\underbrace{\omega\overline{\omega}}_{=1}} = \overline{\omega} \in \mathbb{Z}[\omega]$, also ist ω eine Einheit.

Die anderen Fälle gehen genauso.

zu (A.) c) z.z.: $(1-\omega)^2 \mid 3$: siehe Teil (a)

$$(1-\omega)^2 = 1-2\omega+\omega^2 \overset{\omega^2=-\omega-1}{=} 1-2\omega-\omega-1 = -3\omega$$

$$\Rightarrow \frac{3}{(1-\omega)^2} = \frac{3}{-3\omega} = -\frac{1}{\omega} = -\frac{\overline{\omega}}{\underbrace{\omega\overline{\omega}}_{=1}} = -\overline{\omega} = -\frac{1}{2}(-1-i\sqrt{3}) = \frac{1}{2}(1+i\sqrt{3})$$

$$= \frac{1}{2}(-1+i\sqrt{3})+1 = \omega+1 \in \mathbb{Z}[\omega].$$

(B.) Finde alle $n \in \mathbb{Z}^+$ mit $\varphi(5n) = 5\varphi(n)$. Wir wissen: $\varphi(n) = n \cdot \prod_{\substack{p \in \mathbb{P} \\ p \mid n}} (1-\frac{1}{p})$.

Fall 1: $5 \nmid n$. Dann gilt $\varphi(5n) = 5n \prod_{p \mid 5n}(1-\frac{1}{p}) = \frac{4}{5} \cdot 5n \prod_{p \mid n}(1-\frac{1}{p}) = 4\varphi(n) \neq 5\varphi(n)$.

Fall 2: $5 \mid n$. Dann gilt $\varphi(5n) = 5n \prod_{p \mid 5n}(1-\frac{1}{p}) = 5n \prod_{p \mid n}(1-\frac{1}{p}) = 5\varphi(n)$.

Also gilt $\varphi(5n) = 5\varphi(n) \iff 5 \mid n$.

(6.) w.w.: $\forall n \in \mathbb{N}\ \forall p \in \mathbb{P}$: $v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$.

a) Auf wieviele Nullen endet $(169!)^2$?

Auf soviele, wie $169!$ den Primfaktor 10 enthält – also $\min\{v_2(169!), v_5(169!)\}$ mal.

$$v_2(169!) = \sum_{k \geq 1} \left\lfloor \frac{169}{2^k} \right\rfloor = \sum_{k=1}^{7} \left\lfloor \frac{169}{2^k} \right\rfloor = 84+42+21+10+5+2+1 = 165,$$

$$v_5(169!) = \sum_{k=1}^{3} \left\lfloor \frac{169}{5^k} \right\rfloor = 33+6+1 = 40, \text{ also auf 40 Nullen.}$$

b) z.z.: $\sqrt[n]{n!} \leq \prod_{p \mid n!} p^{\frac{1}{p-1}}$

$$\sqrt[n]{n!} = \sqrt[n]{\prod_{p \mid n} p^{v_p(n!)}} \leq \sqrt[n]{\prod_{p \mid n!} p^{\sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor}} = \prod_{p \mid n!} p^{\frac{\sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor}{n}}.$$

Nun gilt $\sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor \leq n \sum_{k \geq 1} \left(\frac{1}{p}\right)^k = n\left(\frac{1}{1-\frac{1}{p}} - 1\right) = n\left(\frac{1}{p-1}\right)$ also

$\frac{\sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor}{n} \leq \frac{1}{p-1}$ und daher die gewünschte Ungleichung. □

(2.) Seien $a, b \in \mathbb{Z}^+$ mit $a \mid b^2$, $b^2 \mid a^3$, $a^3 \mid b^4$, ... z.z.: $a = b$.

Sei $a = \prod_{p \in \mathbb{P}} p^{v_p(a)}$, $b = \prod_{p \in \mathbb{P}} p^{v_p(b)}$, dann gilt für jedes $p \in \mathbb{P}$:

$v_p(a) \leq v_p(b^2) \leq v_p(a^3) \leq v_p(b^4) \leq \dots$ bzw. äquivalent dazu

$v_p(a) \leq 2v_p(b) \leq 3v_p(a) \leq 4v_p(b) \leq \dots$

Wir zeigen nun $v_p(a) = v_p(b)$. Gilt $v_p(b) = 0$, folgt $v_p(a) = 0$ und wir sind fertig. Andernfalls gilt $\forall n \geq 3$: $(n-1)v_p(b) \leq n v_p(a) \leq (n+1)v_p(b)$, also

$$\frac{n-1}{n} \leq \frac{v_p(a)}{v_p(b)} \leq \frac{n+1}{n},$$

woraus mit dem Einschließsatz für $n \to \infty$ $v_p(a) = v_p(b)$ folgt. □

(4.) z.z.: $n \geq 1 \Rightarrow (n! + 1, (n+1)! + 1) = 1$.

Ang., es gäbe ein $p \in \mathbb{P}$ mit $p \mid (n!+1) \wedge p \mid ((n+1)! + 1)$.

Dann gilt auch $p \mid (n+1)! + 1 - (n!+1) = n! \, n$

und somit, wegen $p \in \mathbb{P}$, $p \leq n$. Damit erhalten wir aber $p \mid n!$, im Widerspruch zu $p \mid (n! + 1)$. □

(3.) z.z.: $H_n = \sum_{k=1}^{n} 1/k \notin \mathbb{Z}$ für $n > 1$.

Es gilt $H_n = \left(\sum_{k=1}^{n} \frac{kgV(1,\dots,n)}{k} \right) / kgV(1,\dots,n)$. Wir zeigen, dass dieser Bruch die Form ungerade / gerade hat und folglich nicht ganzzahlig ist.

Seien dazu $d \in 2\mathbb{N}+1$ und $t \in \mathbb{N}$ mit $kgV(1,\dots,n) = 2^t d$ sowie $s := \max\{m \in \mathbb{N} : 2^m \leq n\}$.

Offensichtlich gilt $t = s$. Nun gilt

$$\frac{kgV(1,\dots,n)}{k} \in \begin{cases} 2\mathbb{N}+1, & k = 2^s \\ 2\mathbb{N}, & k \neq 2^s. \end{cases}$$

Der Zähler hat also genau einen ungeraden Summanden und ist daher ungerade.

Der Nenner ist für $n > 1$ offenbar gerade. □

(8.) z.z.: $s \notin \mathbb{P} \Rightarrow 2^s - 1 \notin \mathbb{P}$.

Sei $s = ak$, $a, k > 1$. Dann gilt $2^{s-1} = 2^{ak} - 1 = \underbrace{(2^a - 1)}_{p} \underbrace{\left(\frac{2^{ak} - 1}{2^a - 1} \right)}_{q}$

und $q = \frac{(2^a)^k - 1}{2^a - 1} = \sum_{i=1}^{k} (2^a)^{i-1} \in \mathbb{N}$, also $2^{s-1} = p \cdot q$ mit $p, q > 1$. □