Aufgabe 3

Wir zeigen zunächst, dass $\mathbb{Z}[i]$ eine Untergruppe von $\mathbb{C}$ ist:

- Offenbar gilt $0 = 0 + i \cdot 0 \in \mathbb{Z}[i]$
- Sind $a+ib,\ a'+ib' \in \mathbb{Z}[i]$, also $a, a', b, b' \in \mathbb{Z}$, so auch $(a+ib)+(a'+ib') = \underbrace{a+a'}_{\in \mathbb{Z}} + i\underbrace{(b+b')}_{\in \mathbb{Z}}$
- Ist $a+ib \in \mathbb{Z}[i]$, also $a, b \in \mathbb{Z}$, so sind auch $-a, -b \in \mathbb{Z}$ und somit $-(a+ib) = -a + i(-b) \in \mathbb{Z}[i]$

0,5 # Pkte

Da $\mathbb{C}\ (= (\mathbb{C}, +))$ abelsch ist, ist auch $\mathbb{Z}[i]\ (= (\mathbb{Z}[i], +))$ abelsch.

Genauso übertragen sich die Assoziativität (und Kommutativität) der Multiplikation und die Distributivität direkt von der Obermenge:

gelten für alle Elemente der Obermenge, insbes. auch für die der Teilmenge

Da $1 = 1 + i \cdot 0 \in \mathbb{Z}[i]$, ist $\mathbb{Z}[i]$ also ein Unterring von $\mathbb{C}$

0,5 Pkte

Nun zeigen wir, dass ein Element $a+ib \in \mathbb{Z}[i]$ genau dann eine Einheit ist, falls $\|a+ib\| = 1$ ist:

Ist $a+ib \in \mathbb{Z}[i]^\times$, so ex. ein $\underbrace{z}_{a'+ib'} \in \mathbb{Z}[i]$ mit

$(a+ib)z = 1 = z(a+ib)$.

1 Pkt

Somit erhalten wir

$\|(a+ib)z\| = \|1\| = 1$

$= \|a+ib\| \cdot \|z\|$

$= \sqrt{a^2+b^2} \cdot \sqrt{a'^2+b'^2}$

und daher

$(a^2+b^2)(a'^2+b'^2) = 1.$

$\in \mathbb{Z}_{\geq 0}$ $\in \mathbb{Z}_{\geq 0}$

Also $a^2+b^2 = 1 = (a'^2+b'^2)$ und somit $\|a+ib\| = \sqrt{a^2+b^2} = 1.$

(*) Ist $a+ib \in \mathbb{Z}[i]$ mit $\|a+ib\| = 1$, also $\underbrace{a^2+b^2}_{\in \mathbb{Z}_{\geq 0}} = 1$, so muss entweder

- $a \in \{\pm 1\}$, $b = 0$

oder

- $a = 0$, $b \in \{\pm 1\}$

gelten. Somit $a+ib \in \{\pm 1, \pm i\} \subset \mathbb{Z}[i]^\times$.

$1^2 = 1$
$(-1)^2 = 1$
$i(-i) = 1 = (-i)i$

1 Pkt

Tatsächlich haben wir bereits $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ gezeigt, da wir soeben gezeigt haben, dass jedes Element $z \in \mathbb{Z}[i]^\times$ Betrag 1 besitzt und somit wir in (*) zu sehen ist bereits in $\{\pm 1, \pm i\}$ enthalten sein muss. Es gibt also 4 Einheiten in $\mathbb{Z}[i]$

1 Pkt

Die Verknüpfungstabelle von $\mathbb{Z}[i]^\times$ ist

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

1 Pkt

, sodass $\mathbb{Z}[i]^\times$ nach dem letzten Blatt isomorph zu $\mathbb{Z}/4\mathbb{Z}$ ist

(Ein Isomorphismus ist durch

$\mathbb{Z}[i]^\times \to \mathbb{Z}/4\mathbb{Z}$

$i^k \mapsto [k]$

gegeben.)

Aufgabe 4

Schritt 1:

Die Abbildung

$f: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/(nm)\mathbb{Z}, ([x],[y]) \mapsto [xm+yn]$

ist wohldefiniert:

Seien $[x] \in \mathbb{Z}/n\mathbb{Z}$ und $[y] \in \mathbb{Z}/m\mathbb{Z}$ und seien x' bzw. y' andere Repräsentanten von $[x]$ bzw. $[y]$. Es seien also

$x - x' = na \quad (\rightsquigarrow x' = x - na)$

und

$y - y' = mb \quad (\rightsquigarrow y' = y - mb)$

für geeignete $a, b \in \mathbb{Z}$. Somit erhalten wir

$$f([x'],[y']) = [x'm + y'n] = [(x-na)m + (y-mb)n]$$
$$= [xm - nam + yn - mbn]$$
$$= [xm + yn - (nm)(a+b)]$$
$$= [xm+yn] - \underbrace{[(nm)(a+b)]}_{=[0]}$$
$$= [xm+yn],$$

so dass f wohldefiniert ist.

1 Pkt.

Schritt 2:

Die Abbildung f ist ein Gruppenhomomorphismus:

Sind $[x],[x'] \in \mathbb{Z}/n\mathbb{Z}$ und $[y],[y'] \in \mathbb{Z}/m\mathbb{Z}$, so erhalten wir

$$f(([x],[y]) + ([x'],[y'])) = f([x+x'],[y+y'])$$
$$= [(x+x')m + (y+y')n]$$
$$= [xm + yn + x'm + y'n]$$
$$= [xm+yn] + [x'm+y'n]$$
$$= f([x],[y]) + f([x'],[y']).$$

1 Pkt

Schritt 3:

Die Abbildung f ist für teilerfremde n, m injektiv:

Sei $([x],[y]) \in \ker(f)$, d.h. es ex. ein $a \in \mathbb{Z}$ mit

$xm + yn = nma.$

Dann erhalten wir

$xm = n(ma - y)$ und $yn = m(na - x)$,

1 Pkt

sodass n ein Teiler von xm und m ein Teiler von yn ist. Sind n und m nun teilerfremd, so muss also n ein Teiler von x und m ein Teiler von y sein, sodass

$([x],[y]) = ([0],[0]) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Somit ist f für teilerfremde n und m injektiv.

Schritt 4: für teilerfremde n, m

Die Abbildung f ist sogar ein Gruppenisomorphismus:

Da f ein Gruppenhomomorphismus ist, welcher für teilerfremde n und m injektiv ist, müssen wir nur noch begründen, dass f dann auch surjektiv ist. Dies ist der Fall, da $\#(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) = nm = \#(\mathbb{Z}/nm\mathbb{Z})$, und die Begriffe "injektiv" und "surjektiv" für endliche Mengen gleicher Kardinalität zusammenfallen.

1 PL

Die Behauptung folgt nun, da $[1] \in \mathbb{Z}/nm\mathbb{Z}$ für teilerfremde n und m ein Urbild unter f haben muss. Es ex. also $x', y \in \mathbb{Z}$ mit

$mx' + ny = 1 + (nm)q$

für ein geeignetes $q \in \mathbb{Z}$. Somit

$\underbrace{m(x' - nq)}_{=: x} + ny = 1.$

Im Bsp.:

$\underbrace{(-3)\cdot 17}_{<-S1} + \underbrace{4 \cdot 13}_{S2} = 1$

1 PL