F24-T1-A3

a) Sei R ein kommutativer Ring. Ein Element $x \in R$ heißt idempotent, falls es ein $k \in \{1, 2, 3, ...\}$ gibt mit $x^k = 0$. Sei $I \subset R$ ein Primideal und $x \in R$ nilpotent. Zeigen Sie $x \in I$.

b) Sei $I = (1 + i)$ das von $1 + i$ erzeugte Ideal im Ring $\mathbb{Z}[i]$. Zeigen sie, dass der Rinf $\mathbb{Z}[i]/I$ genau zwei Elemente hat.

c) Seien R ein Integritätsbereich und $a, b, c \in R$. Zeigen Sie: Erzeugen a und b in R das Einsideal und ist a ein Teiler von bc, so ist a ein Teiler von c.

Lösung

a) Da $x \in R$ nilpotent ist, gibt es ein $k > 0$, dass $x^k \in I$. Aus der Eigenschaft, dass I ein Primideal in R ist, folgt, da $x^k = x^{k-1}x$, dass x^{k-1} oder x in I liegen muss. Für den Fall das $x \in I$ gilt sind wir fertig, für den anderen Fall macht man das nochmal, also $x^{k-1} = x^{k-2}x$. Induktiv folgt also schließlich, dass $x \in I$ gilt.

b) Wir nennen den Ring $\mathbb{Z}[i] =: S$. Wir betrachten den Homomorphismus

$$\alpha : \mathbb{Z}[i] \to \mathbb{F}_2, \quad a + bi \mapsto [a - b].$$

Dies ist ein Homomorphismus, denn $\alpha((a + bi)(c + di)) = \alpha(ac - bd + i(bc + ad)) = [ac - bd - bc - ad] = [ac + bd - bc - ad] = [a - b][c - d]$ und $\alpha(a + bi + c + di) = \alpha(a + c + i(b + d)) = [a+c-b-d] = [a-b]+[c-d]$. α ist surjektiv, denn $\alpha(1) = [1]$ und $\alpha(0) = [0]$. Wir behaupten noch $\ker(\alpha) = (1+i)$. Sei $a+bi \in (1+i)$, dann ist $a+bi = (c+di)(1+i) = c+ic+id-d = c-d+i(c+d)$. Es gitl also $\alpha(a + bi) = [c - d - (c + d)] = [0]$. Ist $a + bi \in \ker(\alpha)$ so gilt $[a] = [b] \in \mathbb{F}_2$. Es gilt also $a = b + 2k$ mit $k \in \mathbb{Z}$. Es gilt also $a + bi = b + 2k + bi = b(1 + i) + 2k$. Da $(1 - i)(1 + i) = 2$ ist 2 im Ideal $(1 + i)$ und deshalb auch $2k$. Somit gilt $a + bi \in (1 + i)$. Nach dem Homomorphiesatz erhält man schließlich, dass $\mathbb{Z}[i]/I \cong \mathbb{F}_2$ und damit die Behauptung.

c) Aus $(1) = (a, b)$ folgt, dass es $x, y \in R$ gibt, so dass $1 = ax + by$ gilt. Ist nun a ein Teiler von bc so existiert ein $l \in R$ mit $al = bc$. Es folgt also $byc = aly$ und mit $by = 1 - ax$ also $c(1 - ax) = byc = aly$. Wir erhalten schließlich

$$c - acx = aly \Rightarrow c = aly + acx \Rightarrow c = a(ly + cx) \Rightarrow a \mid c.$$