H10-T1-A3

Sei ω eine primitiv dritte Einheitswurzel über $\mathbb{Q}$. Der Ring $R = \mathbb{Z}[\omega]$ ist ein Euklidischer Ring mit Normabbildung $N\colon R \to \mathbb{N}_0$ definiert durch

$$N(a+b\omega) = (a+b\omega)(a+b\omega^2) = a^2 - ab + b^2, \quad a, b \in \mathbb{Z}.$$

Zeigen Sie:

a) Ein Element $y \in R$ ist eine Einheit in $R \Leftrightarrow N(y) = 1$.

b) Sei $p \in \mathbb{Z}$ eine Primzahl. Dann ist $p = a^2 - ab + b^2$ für geeignete $a, b \in \mathbb{Z}$ genau dann, wenn das Ideal $(p) \subset R$ kein Primideal ist.

c) Sei $p \in \mathbb{Z}$ eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der endliche Körper mit p Elementen. Das Ideal $(p) \subset R$ ist genau dann ein Primideal, wenn das Polynom $X^2 + X + 1 \in \mathbb{F}_p[X]$ irreduzibel ist.

Lösungsvorschlag. Zu a). Nach Definition ist $N(z) = z\overline{z}$, wenn $\overline{(\bullet)}$ die komplexe Konjugation bezeichnet (es ist ja gerade $\omega^2 = \overline{\omega}$). Da die komplexe Konjugation multiplikativ ist, ist also auch die gegebene Norm multiplikativ und es gilt $y\overline{y} = N(y) = 1 \Rightarrow R \ni \overline{y} = y^{-1}$, also $y \in R^\times$. Existiert umgekehrt ein z mit $zy = 1$, so folgt $1 = N(1) = N(yz) = N(y)N(z)$, also insbesondere $N(y) = 1$ wegen $N(y), N(z) \in \mathbb{N}$.
Zu b). Bekanntlich ist (p) genau dann ein Primideal, wenn p prim in R ist. Ist $p = a^2 - ab + b^2$ für gewisse $a, b \in \mathbb{Z}$, so setzen wir $z := a + b\omega$ und es ist also $z\overline{z} = N(z) = p = N(\overline{z})$ nach Voraussetzung. Insbesondere sind z und $\overline{z}$ irreduzibel (also prim, da R Euklidisch ist) da aufgrund der Multiplizität der Norm aus Teil a) eine Faktorisierung in R einer Faktorisierung von p in $\mathbb{N}$ entspräche — und es ist $p = z\overline{z}$, somit ist p nicht irreduzibel, also nicht prim.

Ist umgekehrt p nicht prim, so lässt sich p als geeignetes Produkt $p = xy$ schreiben, mit $x, y \in R$ und $N(x) \neq 1 \neq N(y)$ (da p insbesondere nicht irreduzibel ist). Wegen $N(x)N(y) = N(xy) = N(p) = p^2$ muss also gelten $N(x) = p = N(y)$. Ist $x = a + b\omega$ bedeutet dies gerade

$$p = N(x) = a^2 - ab + b^2.$$

Zu c). Da ω eine primitive dritte Einheitswurzel ist (also $\omega^2 + \omega + 1 = 0$ erfüllt), ist der Morphismus von Ringen

$$\mathbb{Z}[\omega] \to \mathbb{F}_p[X]/(X^2 + X + 1), \quad \omega \mapsto X,$$

wohldefiniert. Der Morphismus ist außerdem offensichtlich surjektiv, und sein Kern ist gerade das Ideal (p). Nach dem Homomorphiesatz erhalten wir also einen Isomorphismus

$$R/(p) \xrightarrow{\sim} \mathbb{F}_p[X]/(X^2 + X + 1).$$

Somit ist (p) ein Primideal genau dann, wenn $R/(p)$ ein Integritätsbereich ist, was nun wiederum genau dann der Fall ist, wenn $\mathbb{F}_p[X]/(X^2 + X + 1)$ ein Integritätsbereich ist, was genau dann zutrifft, wenn $(X^2 + X + 1)$ ein Primideal ist, was genau dann so ist, wenn $X^2 + X + 1$ irreduzibel in $\mathbb{F}_p[X]$ ist.