F24-T2-A1

a) Bestimmen Sie eine Zerlegung des Elements $z = 29 \in \mathbb{Z}[i]$ in Primelemente.

b) Es sei $p > 3$ eine Primzahl. Zeigen Sie, dass es in der multiplikativen Gruppe $\mathbb{F}_{p^2}^\times$ ein Element a der Ordnung 12 gibt.

c) Entscheiden Sie, ob $\overline{437} \in \mathbb{Z}/911\mathbb{Z}$ invertierbar ist. Bestimmen Sie gegebenenfalls das Inverse.

d) Entscheiden Sie begründet, ob $\mathbb{R}$ eine algebraische Erweiterung von Grad 4 hat.

Lösung

a) Es gilt $(5+2i)(5-2i) = 29 \in \mathbb{Z}[i]$. Jetzt wollen wir sehen, dass $(5 \pm 2i)$ Primelemente in $\mathbb{Z}[i]$ sind. Dazu benutzen wir das wir wissen, dass $\mathbb{Z}[i]$ ein euklidischer Ring ist und demnach faktoriell. Es reicht also zu zeigen, dass $(5 \pm 2i)$ irreduzibel in $\mathbb{Z}[i]$ ist. Wir betrachten dazu die multiplikative Normabbildung

$$N : \mathbb{Z}[i] \to \mathbb{N}, \quad (a + bi) \mapsto a^2 + b^2.$$

Wir benutzen, dass diese multiplikativ ist und, dass für Einheiten x in $\mathbb{Z}[i]$ gilt, dass $N(x) = 1$ gilt und umgekehrt. $N(5 \pm 2i) = 29$. 29 ist prim, daher gibt es keine nichtriviale Zerlegung von $5 \pm 2i$ in $\mathbb{Z}[i]$, denn sonst gäbe es auch eine nichttriviale Zerlegung von $29 \in \mathbb{N}$ ein Widerspruch. Also ist $5 \pm 2i$ irreduzibel in $\mathbb{Z}[i]$.

b) Da $\mathbb{F}_{p^2}$ ein Körper ist hat dessen Einheitengruppe $p^2 - 1$ Elemente. Zudem ist die Einheitengruppe eines Körpers stets zyklische. Wir betrachten also fortan die Gruppe $\mathbb{Z}/p^2 - 1\mathbb{Z}$. Es gilt nach der dritten binomischen Formel:

$$p^2 - 1 = (p - 1)(p + 1).$$

Da $p > 3$ eine Primzahl ist, ist sowohl $p + 1$ als auch $p - 1$ gerade, es folgt also $4 \mid (p^2 - 1)$. Wiederum mit $p > 3$ Primzahl folgt, dass 3 nicht p teilt, es muss also $p-1$ oder $p+1$ teilen, denn genau eine von drei aufeinanderfolgenden ganzen Zahlen ist immer durch 3 teilbar. Folglich ist $p^2 - 1$ durch 3 teilbar und da $\mathrm{ggT}(3, 4) = 1$ ist $p^2 - 1$ durch 12 teilbar. Da $\mathbb{F}_{p^2}^\times$ zyklisch ist gibt es also genau eine zyklische Untergruppe der Ordnung 12. Dessen Erzeuger hat Ordnung 12.

c) Wir berechnen dazu $\mathrm{ggT}(437, 911)$ mit Hilfe des euklidischen Algortithmus. Es gilt

$$911 = 2 \cdot 437 + 37.$$

Weiter gilt

$$437 = 11 \cdot 37 + 30.$$

Im nächsten Schritt bekommt man

$$37 = 1 \cdot 30 + 7.$$

Und schließlich

$$30 = 4 \cdot 7 + 2$$

und

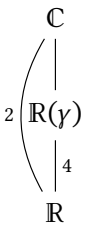
$$7 = 3 \cdot 2 + 1.$$

Es gilt also $\mathrm{ggT}(911, 437) = 1$.
Geht man die Schritte nun rückwärts durch, so erhält man folgende Darstellung der 1:

$$189 \cdot 911 - 394 \cdot 437 = 1.$$

Folglich ist $\overline{-394} = \overline{517}$ das Inverse von $\overline{437}$ in $\mathbb{Z}/911\mathbb{Z}$.

d) Nein. Angenommen die gäbe es. Sei also $L|\mathbb{R}$ eine solche algebraische Erweiterung von Grad 4. Da $\mathrm{char}(\mathbb{R}) = 0$ ist diese Körpererweiterung separabel. Nach dem Satz vom primitiven Element gibt es jetzt ein $\gamma \in \mathbb{C}$, so dass $L = \mathbb{R}(\gamma)$. Jetzt folgt aber damit, dass $L \subset \mathbb{C}$. Wir haben also folgende Situation:



Das ergibt offenbar einen Widerspruch ($4 \nmid 2$).