Algebra

Übungsblatt 10

Prof. Dr. Fabien Morel
Dr. Maksim Zhykhovich WiSe 2019/2020
23.12.2019

Aufgabe 1. Sei $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$.
Zeige: $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2 + 1)$ als Ringe.

Aufgabe 2. Seien K ein Körper und $n, m \in \mathbb{N}$.
(1) Zeige: Der Rest der Euklidischen Division von $X^n - 1$ durch $X^m - 1$ in $K[X]$ ist $X^r - 1$, wobei $r \in \mathbb{N}$ der Rest der Euklidischen Division vom n durch m in $\mathbb{Z}$ ist.
(2) Folgere: $X^m - 1 \mid X^n - 1$ in $K[X]$ genau dann wenn $m|n$ in $\mathbb{Z}$.

Aufgabe 3. Sei π ein irreduzibles Element in $\mathbb{Z}[i]$.
Zeige: Bis auf Einheiten ist π entweder eine Primzahl aus $\mathbb{Z}$ oder von der Form $a + bi \in \mathbb{Z}[i]$, für die $a^2 + b^2$ eine Primzahl aus $\mathbb{Z}$ ist.
Hinweis: Benutze dass $\mathbb{Z}[i]$ ein Hauptidealring und dann auch ein faktorieller Ring ist.

Aufgabe 4. (1) Sei p eine Primzahl.
Zeige: Es existiert kein $x \in \mathbb{F}_p$ mit $x^2 = -1$ genau dann wenn $p \equiv 3 \bmod 4$.
Hinweis: Benutze dass $x^{p-1} = 1$ für alle $x \in \mathbb{F}_p^*$ gilt und auch Aufgabe 2.2, Übungsblatt 8.
(2) Sei p eine Primzahl aus $\mathbb{Z}$ von der Form $p \equiv 3 \bmod 4$.
Zeige: p ist auch ein Primelement in $\mathbb{Z}[i]$.
Hinweis: Man beobachtet dass $N(z_1 z_2) = N(z_1)N(z_2)$ für alle $z_1, z_2 \in \mathbb{Z}[i]$ gilt, wobei $N(a + bi) = a^2 + b^2$. Benutze auch die Frage (1).
(3) Sei p eine Primzahl aus $\mathbb{Z}$ von der Form $p \equiv 1 \bmod 4$ oder $p = 2$.
Zeige: p ist nicht prim in $\mathbb{Z}[i]$ und es gibt $a, b \in \mathbb{Z}$ mit $p = a^2 + b^2$.
Hinweis: Benutze die Frage (1) und wähle $m \in \mathbb{Z}$ mit $m^2 \equiv -1 \bmod p$, sodass $m^2 + 1 = pl$. Bemerke dass $m^2 + 1 = (m + i)(m - i)$ in $\mathbb{Z}[i]$.