VU Discrete Mathematics

Exercises for 25th November 2025

37) Let G be a finite, abelian group and $a \in G$ an element for which $\operatorname{ord}_G(a)$ is maximal. Prove that for all $b \in G$ the order $\operatorname{ord}_G(b)$ is a divisor of $\operatorname{ord}_G(a)$.

38) Show that $m \mid n$ implies $\lambda(m) \mid \lambda(n)$ where λ denotes the Carmichael function.

Hint: Prove first that $a_i \mid b_i$ for $i = 1, \ldots, k$ implies $\operatorname{lcm}(a_1, a_2, \ldots, a_k) \mid \operatorname{lcm}(b_1, b_2, \ldots, b_k)$.

39) Let $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ where $i = \sqrt{-1}$. Show that $\mathbb{Z}[i]$ is a subring of $(\mathbb{C}, +, \cdot)$ and determine its group of units $(\mathbb{Z}[i]^*, \cdot)$. Is $\mathbb{Z}[i]$ an integral domain?

40) Determine a greatest common divisor of $13 - 2\sqrt{2}i$ and $3 + 9\sqrt{2}i$ in $\mathbb{Z}[i\sqrt{2}] = \{a + bi\sqrt{2} \mid a, b \in \mathbb{Z}\}$.
Hint: $\mathbb{Z}[i\sqrt{2}]$ is a Euclidean ring with Euclidean function $n(a + bi\sqrt{2}) = a^2 + 2b^2$. (You are not asked to prove that!) In order to find q, r in $u = qv + r$, determine $\frac{u}{v}$ in $\mathbb{Z}[i\sqrt{2}]$ and round the real part and the coefficient of $i\sqrt{2}$.

41) Let $(R, +, \cdot)$ be a Euclidean ring and let its Euclidean function be denoted by n. Show that $n(x) = n(1)$ for all $x \in R^*$. Prove moreover that, if $x \in R$ and $y \in R^*$, then $n(xy) = n(x)$.

42) Consider the ring $R = \mathbb{Z}[i\sqrt{3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$.

a) Prove that 1 is a greatest common divisor of $1 + i\sqrt{3}$ and $1 - i\sqrt{3}$).

b) Prove that $\gcd(2 + 2i\sqrt{3}, 4)$ does not exist.

c) Prove that there is no $a \in R$ with $a^2 = 1 + i\sqrt{3}$.