VU Discrete Mathematics

Exercises for 2nd December 2025

43) Let R be a ring and I be an ideal of R. Then $(R/I, +)$ is the quotient group of $(R, +)$ over $(I, +)$. Define a multiplication on R/I by

$$(a + I) \cdot (b + I) := (ab) + I.$$

Prove that this operation is well-defined, *i.e.* that

$$\left.\begin{array}{rr} & a + I = c + I \\ \text{and} & b + I = d + I \end{array}\right\} \implies (ab) + I = (cd) + I.$$

Furthermore, show that $(R/I, +, \cdot)$ is a ring.

44) Prove: If a is a prime element of an integral domain R, then the quotient ring $R/(a)$ has no zero divisors.

45) Let K be a field and $p(x) \in K[x]$ a polynomial of degree m. Prove that $p(x)$ cannot have more than m zeros in K (counted with multiplicities).
Use this result to prove that for any prime number p the relation $(p-1)! \equiv -1 \ (p)$ holds.

Hint: Use the fact that $K[x]$ is a unique factorization domain.

46) Show that in the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ an element $a + bi$ is irreducible, if $a^2 + b^2$ is irreducible in $\mathbb{Z}$. Furthermore, prove that for every prime number p there is at most one decomposition $p = a^2 + b^2$ with $a, b \in \mathbb{N}$ up to the order of the summands.

Hint: Note that $a^2 + b^2 = (a + bi)(a - bi)$.

47) Let $\varphi : R_1 \to R_2$ be a ring homomorphism and I be an ideal of R_2. Prove that $\varphi^{-1}(I) := \{x \in R_1 \mid \varphi(x) \in I\}$ is an ideal of R_1.

48) Using the definition of ideals, prove that $I = \{(x^2 + 1) \cdot p(x) \mid p(x) \in \mathbb{R}[x]\}$ is an ideal of $\mathbb{R}[x]$. Moreover, prove directly (i.e., without using congruences) that $x^2 + I = -1 + I$ holds and that $\mathbb{R}[x]/I \cong \mathbb{C}$.