Algebra exam, sample, 2025

Formulate claims and definitions including all assumptions. Write proofs in the same formal way as in the lecture notes. Justify your answers and, if you use a non-trivial claim from the lecture in your argument, formulate it.

(1) Formulate and prove the Chinese remainder theorem for integers.

(10 points)

(2) Prove that polynomial ring $\mathcal{R}[x]$ over a domain $\mathcal{R}$ is a domain. Does exist a field $\mathcal{F}$ such that $\mathcal{F}[x]$ is a field? Explain your claim.

(10 points)

(3) Show that $m(\alpha) = \alpha^3+\alpha+1$ is irreducible in the domain $\mathbb{Z}_7[\alpha]$. Solve the equation $(\alpha^2+3)x + \alpha + 4 = \alpha^2$ in the field $\mathbb{Z}_7[\alpha]/(m(\alpha))$.

(10 points)

(4) Define the notion of a group and its subgroup. If $(G, \cdot, ^{-1}, 1)$ is an abelian group, prove for each $n \in \mathbb{N}$ that $\{g^n \mid g \in G\}$ is a carrier set of a subgroup of $(G, \cdot, ^{-1}, 1)$.

(10 points)

(5) What is a discrete logarithm? Describe El Gamal encyption. Let $G = \mathbb{Z}_{17}^* = \langle 3 \rangle$ is a cyclic group and $k = 7$ is a secret key. Encrypt the message 12 using El Gamal protocol.

(10 points)